FHZ —> FACHHOCHSCHULE ZENTRALSCHWEIZ

HSLU

IWI —> INSTITUT FÜR
WIRTSCHAFTSINFORMATIK LUZERN

ANALYSE DER ZUSATZFUNKTIONALITÄTEN VERSCHIEDENER FIREWALLS

DIPLOMARBEIT

Nachdiplomstudium
Informatiksicherheit

eingereicht an der

Fachhochschule Zentralschweiz
Hochschule für Wirtschaft
Institut für Wirtschaftsinformatik
Luzern

vorgelegt von

Tom Schmidt

Referent:

Roland Portmann

Korreferent:

David Hyams

Diese Arbeit ist nicht vertraulich

2003

INHALTSVERZEICHNIS

MANAGEMENT SUMMARY 5
1. EINLEITUNG 6
1.1 ZIELE UND UMFANG DER DIPLOMARBEIT 6
1.2 GRUND- VERSUS ZUSATZFUNKTIONALITÄT EINER FIREWALL 6
1.3 ABGRENZUNGEN 7
1.4 VORGEHENSWEISE 7
1.5 VERWENDETE SYMBOLIK 8
2. MÖGLICHE ZUSATZFUNKTIONALITÄTEN VON FIREWALLS 10
2.1 AUTHENTISIERUNGSMÖGLICHKEITEN 10
2.2 ZEITEINSCHRÄNKUNG EINZELNER FIREWALL-REGELN 10
2.3 URL-FILTERING, URL-BLOCKING 11
2.4 CONTENT-FILTERING 11
2.5 VIRENPRÜFUNG 11
2.6 SMTP-FILTERING 12
2.7 SPAM-FILTERING 12
2.8 „INTRUSION DETECTION"-FUNKTIONEN 12
2.9 ANTI-SPOOFING (IP-SPOOFING) 12
2.10 ÜBERWACHUNG DER INTERNETAKTIVITÄTEN 13
2.11 ERWEITERTE LOGGING-MÖGLICHKEITEN 13
2.12 ALARMIERUNG 13
2.13 UNTERSTÜTZUNG VON NAT UND/ODER PAT 14
2.14 DHCP-SERVER 14
2.15 ZEITSERVER-DIENST 14
2.16 DYNAMISCHES DNS 15
2.17 WIRELESS-LAN (WLAN) 15
2.18 VIRTUAL PRIVATE NETWORK (VPN) 16
2.19 DIAGNOSE-TOOLS 16
2.20 REMOTE-MANAGEMENT 16
2.21 FIRMWARE- BZW. FIREWALL-UPDATES 17
2.22 DIAL-UP-BACKUP, VERKEHRSUMLEITUNG 17
2.23 BACKUP UND RESTORE DER FIREWALL-KONFIGURATION 17
2.24 HOHE VERFÜGBARKEIT 17
2.25 LASTVERTEILUNG / LOAD BALANCING 18
3. SELEKTIONSKRITERIEN FÜR DIE ZU ANALYSIERENDEN FIREWALLS 19
4. ÜBERSICHT ÜBER DIE FUNKTIONALITÄTEN DER ANALYSIERTEN FIREWALLS 20
4.1 ZYXEL ZYWALL 10W 20
4.2 SONICWALL SOHO3 25-USER MIT VPN 21
4.3 CHECK POINT FIREWALL-1 NEXT GENERATION (NG) 22
5. ZYXEL ZYWALL 10W 23
5.1 ALLGEMEINE HINWEISE ZUR FIREWALL 23
5.2 GRUNDKONFIGURATION UND WESENTLICHE STANDARDEINSTELLUNGEN 24
5.3 ZUSATZFUNKTIONALITÄTEN 25
5.3.1 Content- und URL-Filtering 25
5.3.2 „Intrusion Detection"-Funktionen, Anti-Spoofing 33
5.3.3 Logging-Möglichkeiten und Alarmierung 37

5.3.4 Network Address Translation (NAT) 39
5.3.5 DHCP-Server 40
5.3.6 Zeitserver-Dienst 40
5.3.7 Dynamisches DNS 41
5.3.8 Wireless-LAN (WLAN) 43
5.3.9 Virtual Private Network (VPN) 45
5.3.10 Diagnosemöglichkeiten 49
5.3.11 Remote-Management 49
5.3.12 Firmware-Updates 51
5.3.13 Dial-Up-Backup 51
5.3.14 Verkehrsumleitung 52
5.3.15 Backup und Restore der Firewall-Konfiguration 52
5.3.16 Logische Netzwerksegmente 53
5.3.17 WAN-Protokolle 53

6. SONICWALL SOHO3 25-USER MIT VPN 55

6.1 ALLGEMEINE HINWEISE ZUR FIREWALL 55
6.2 GRUNDKONFIGURATION UND WESENTLICHE STANDARDEINSTELLUNGEN 56
6.3 ZUSATZFUNKTIONALITÄTEN 57
6.3.1 Authentisierungsmöglichkeiten 57
6.3.2 Zeiteinschränkung einzelner Firewall-Regeln 58
6.3.3 Content- und URL-Filtering 59
6.3.4 Virenprüfung 66
6.3.5 „Intrusion Detection“-Funktionen, Anti-Spoofing 68
6.3.6 Logging-Möglichkeiten, Alarmierung und Überwachung der Internetaktivitäten 70
6.3.7 Network Address Translation (NAT) 72
6.3.8 DHCP-Server 73
6.3.9 Zeitserver-Dienst 73
6.3.10 Virtual Private Network (VPN) 75
6.3.11 Diagnosemöglichkeiten 77
6.3.12 Remote-Management 77
6.3.13 Firmware-Updates 78
6.3.14 Backup und Restore der Firewall-Konfiguration 79
6.3.15 Hohe Verfügbarkeit 79
6.3.16 Schutz der Firewall vor Angriffen 80
6.3.17 Logische Netzwerksegmente 81
6.3.18 WAN-Protokolle 81

7. CHECK POINT FIREWALL-1 NEXT GENERATION 83

7.1 ALLGEMEINE HINWEISE ZUR FIREWALL 83
7.2 GRUNDKONFIGURATION UND WESENTLICHE STANDARDEINSTELLUNGEN 84
7.3 ZUSATZFUNKTIONALITÄTEN 85
7.3.1 Authentisierungsmöglichkeiten 86
7.3.2 Zeiteinschränkung einzelner Firewall-Regeln 89
7.3.3 Content-, SMTP- und URL-Filtering 89
7.3.4 „Intrusion Detection“-Funktionen, Anti-Spoofing 92
7.3.5 Erweiterte Logging-Möglichkeiten und Alarmierung 95
7.3.6 Network Address Translation (NAT) 97
7.3.7 Virtual Private Network (VPN) 98
7.3.8 Remote-Management 102
7.3.9 Firewall-Updates 103
7.3.10 Backup und Restore der Firewall-Konfiguration 104

7.3.11 Hohe Verfügbarkeit und Load-Balancing 105

8. GEGENÜBERSTELLUNG DER VERSCHIEDENEN ZUSATZFUNKTIONALITÄTEN 108

9. SCHLUSSBEMERKUNGEN / FAZIT 112

10. QUELLENVERZEICHNIS 113

10.1 LITERATURVERZEICHNIS 113

10.2 VERZEICHNIS VON INTERNETADRESSEN 114

11. VERZEICHNIS DER ABBILDUNGEN UND TABELLEN 117

11.1 ABBILDUNGSVERZEICHNIS 117

11.2 TABELLENVERZEICHNIS 119

12. GLOSSAR 120

13. ANHANG I

13.1 ZYWALL 10W – ALLGEMEINE INTERESSANTE FESTSTELLUNGEN BEZÜGLICH IT-SICHERHEIT I

13.1.1 Versteckte undokumentierte Datei auf Firewall I

13.1.2 DynDNS-Passwort wird nur schwach codiert über das Internet transferiert II

13.1.3 Ergebnisse technische Untersuchungen URL-Filtering ZyWALL 10W IV

13.2 KONFIGURATIONSBEISPIELE VIII

13.2.1 Bridging-Modus-Konfiguration des ZyXEL Prestige 642R ADSL-Routers VIII

13.2.2 ZyWALL 10W – VPN-Einstellungen für die Interoperabilität mit SonicWALL SOHO 3 und Check Point Firewall-1 NG XI

13.2.3 SonicWALL SOHO3 – VPN-Einstellungen für die Interoperabilität mit ZyWALL 10W und Check Point Firewall-1 NG XIII

13.2.4 Check Point Firewall-1 NG – VPN-Einstellungen für die Interoperabilität mit ZyWALL 10 W und SonicWALL SOHO 3 XV

13.2.5 Windows 2000 IPSec – VPN-Client für Firewalls „selbst gemacht“ XVIII

13.2.6 Windows 2000 IPSec – Ergänzungen zum Einrichten des VPN-Clients für Check Point Firewalls XL

Management Summary

Firewalls sind heutzutage in der vernetzten Informationstechnik nicht mehr wegzudenken. Jedes Unternehmen, ungeachtet seiner Grösse, mit einer Anbindung an unsichere öffentliche Netzwerke wie zum Beispiel das Internet implementiert eine Firewall, wenn sein Handeln nicht als fahrlässig eingestuft werden soll.

Seit Anfang der 90er-Jahre, als die ersten modernen Firewalls aufkamen, haben sich die Produkte, insbesondere auch in jüngster Vergangenheit, stark weiterentwickelt. Mittlerweile sind unzählige Firewalls von vielen verschiedenen Herstellern mit den unterschiedlichsten Funktionalitäten erhältlich. Dabei stellt sich die Frage, ob die integrierten Zusatzfunktionalitäten für die durch die Hersteller angestrebten Zielgruppen auch wirklich sinnvoll sind oder ob diese primär aus Marketingüberlegungen implementiert und propagiert werden.

Viele der Zusatzfunktionalitäten sind weder standardisiert noch in ihrer Bezeichnung einheitlich. Aufgrund der Prospekte und des Marketing-Materials der Hersteller kann kaum ein Rückschluss auf die effektive Funktionsweise und den Umfang einer Zusatzfunktionalität gezogen werden.

In der vorliegenden Diplomarbeit wurden die Zusatzfunktionalitäten ausgesuchter Firewalls (ZyXEL ZyWALL 10W, SonicWALL SOHO3 und Check Point Firewall-1 NG) einer eingehenden (je nach Zusatzfunktionalität auch technischen) Analyse unterzogen und beurteilt, ob die Implementation einer Zusatzfunktionalität direkt auf der Firewall überhaupt als sinnvoll erscheint, ob sie den gewünschten und erwarteten Nutzen stiften kann und ob damit eventuell inhärente Sicherheitsrisiken verbunden sind. Insbesondere die Firewalls, welche auf den KMU-Markt abzielen, können in Anbetracht ihres Preises mit einer erstaunlichen Fülle von Funktionen und Zusatzfunktionalitäten aufwarten.

Die Untersuchungen haben ergeben, dass die meisten der Zusatzfunktionalitäten sinnvolle Ergänzungen einer Firewall für das jeweilige Marktsegment darstellen und durchaus Bedürfnisse der Betreiber abdecken können. Bei der Wirksamkeit einiger Zusatzfunktionalitäten wurden jedoch, je nach Hersteller und Art der Implementation, gewisse Defizite festgestellt. Ausserdem beeinflussen manche Zusatzfunktionalitäten die Gesamtsicherheit der Firewall oder des internen Netzwerks negativ, was in Widerspruch zur Kernaufgabe einer Firewall steht.

Auch wenn durch die Aktivierung gewisser Zusatzfunktionalitäten die Sicherheit einer Firewall und des internen Netzwerks verbessert werden kann, bestehen oft Mittel und Wege, diese zusätzlichen Schutzmechanismen gezielt zu umgehen. Auf diese Problematik wird in der vorliegenden Arbeit ebenfalls eingegangen und entsprechende Verfahren werden aufgezeigt. Für die IT-Verantwortlichen eines Unternehmens ist es wichtig, sich dieser Gefahren und der entsprechenden (Rest-)Risiken bewusst zu sein, um weitere gezielte (unter Umständen auch organisatorische) Massnahmen einleiten zu können.

Die vorliegende Arbeit soll IT-Verantwortlichen, Firewall-Administratoren und anderen Interessierten einen praxisnahen gezielten Überblick über die Zusatzfunktionalitäten von Firewalls, deren Wirksamkeit und Einschränkungen und der allfälligen inhärenten Sicherheitsrisiken verschaffen. Dazu dienen auch die sich im Anhang zu dieser Arbeit befindenden Konfigurationsanleitungen zur Einrichtung einiger der Zusatzfunktionalitäten.

1. EINLEITUNG

1.1 Ziele und Umfang der Diplomarbeit

Die vorliegende Diplomarbeit beschäftigt sich mit der Frage, welche Zusatzfunktionalitäten heutzutage verschiedene Firewalls neben ihrer Grundfunktionalität bieten. Es soll anhand ausgewählter Firewall-Produkte untersucht werden, wie die Zusatzfunktionalitäten wirken und ob sie wie vorgesehen wirken, welchen Nutzen sie den Firewall-Betreiber stiften können, ob die Zusatzfunktionalitäten ihrerseits unter Umständen selber zu Sicherheitsrisiken führen könnten und ob diese Erweiterungen aus Sicht des Verfassers der Diplomarbeit überhaupt eine sinnvolle Ergänzung einer Firewall darstellen.

Bei der Diplomarbeit handelt es sich um **keine** Einführung in die Thematik „Firewall“. Der Verfasser geht davon aus, dass die Leser bereits über Firewall-Kenntnisse verfügen, insbesondere dass ihnen die verschiedenen Firewall-Typen wie Paket-Filter, Stateful Inspection, Applikations-Proxy usw. bekannt sind, dass sie wissen, welches die Einsatzgebiete von Firewalls sind und wie eine Firewall grundsätzlich funktioniert. Der Inhalt der vorliegenden Arbeit baut auf diesem Firewall-Grundlagenwissen auf.

Der Fokus der Arbeit wurde absichtlich auf die Zusatzfunktionalitäten von Firewalls und nicht auf deren Grundfunktionalität gelegt (Erläuterungen zur Abgrenzung zwischen Grundfunktionalität und Zusatzfunktionalität einer Firewall folgen unter Kapitel 1.2). Die Grundfunktionalität einer Firewall wird heutzutage von vielen, zum Teil auch unabhängigen, Institutionen getestet und kann bei den bekannten Firewall-Produkten als gegeben angesehen werden. Unter anderem lassen die meisten der bekannten Hersteller ihre Firewalls durch ICSA Labs[1] zertifizieren. So wurden z.B. alle in dieser Diplomarbeit untersuchten Firewalls in der einen oder anderen Version bereits durch diese Zertifizierungsstelle geprüft. Manche Firewalls verfügen zudem über eine Common Criteria[2] Zertifizierung.

Damit sich die Diplomarbeit leichter lesen lässt, sind alle personenbezogenen Bezeichnungen in männlicher Form gehalten. Selbstverständlich gelten diese auch für Personen weiblichen Geschlechts.

1.2 Grund- versus Zusatzfunktionalität einer Firewall

Da es in der Praxis keine offizielle Abgrenzung zwischen Grund- und Zusatzfunktionalität einer Firewall gibt, werden diese beiden Begriffe aus Sicht des Verfassers kurz definiert:

Grundfunktionalität Als Grundfunktionalität einer Firewall wird prinzipiell das korrekte Abarbeiten der Firewall-Regeln angesehen, d.h., es wird von einer Firewall erwartet, dass sie gemäss den erfassten Firewall-Regeln ein Datenpaket entweder blockt oder zulässt. Ausserdem gehört das Erstellen einer rudimentären Log-Datei (Mindestangaben: Datum und Zeit des Ereignisses, betroffene Regel, Quell-Adresse und -Port des Pakets, Ziel-Adresse und -Port des Pakets, Information ob

[1] ICSA Labs, siehe http://www.icsalabs.com
[2] Common Criteria, siehe http://www.commoncriteria.org

Paket geblockt oder zugelassen wurde), welche Hinweise zu den durch den Benutzer definierten Vorfällen enthält, zur Grundfunktionalität.

Zusatzfunktionalität Als Umkehrschluss zur Definition der Grundfunktionalität gehören zur Zusatzfunktionalität einer Firewall alle Eigenschaften, welche nicht als Grundfunktionalität gelten. Dazu zählen zum Beispiel: Alarmierung, Filtern von Verkehr aufgrund der URL oder des Inhalts, Virtual Private Networks (VPNs), Schnittstellen zu anderen Programmen wie Antiviren-Software, Wireless-LAN-Accesspoints usw.

Wann immer in der vorliegenden Diplomarbeit somit von Grund- und Zusatzfunktionalität einer Firewall die Rede ist, gelten die obenstehenden Definitionen.

1.3 Abgrenzungen

Die Untersuchung der Zusatzfunktionalitäten der Firewalls beschränkt sich, wie unter Ziele und Umfang der Diplomarbeit erwähnt, auf die Funktionalität und den damit allenfalls verbundenen Sicherheitsrisiken. Auf rechtliche Aspekte, welche je nach Zusatzfunktionalität (z.B. Aufzeichnen des Internet-Verkehrs auf der Firewall usw.) durchaus relevant werden könnten, wird im Rahmen dieser Diplomarbeit nicht eingegangen.

Es wird auch nicht untersucht, welche Performance-Auswirkungen der Einsatz solcher Zusatzfunktionalitäten auf die Firewall und auf das Netzwerk hat. Solche Last- und Performance-Tests, welche sinnvollerweise eine statistisch erhärtete Aussage liefern können, sind nur mittels grossem Zeitaufwand und unter Einsatz einer entsprechenden Infrastruktur, in welcher das Verhalten auch realistisch gemessen und eruiert werden kann, möglich. Da im Rahmen dieser Diplomarbeit die dazu nötigen Voraussetzungen nicht vorhanden sind, wird darauf verzichtet.

1.4 Vorgehensweise

Die in der vorliegenden Arbeit gemachten Aussagen basieren mehrheitlich auf ausgewählten Tests der Zusatzfunktionalitäten der entsprechenden Firewall-Produkte. Alle untersuchten Produkte wurden von Grund auf installiert und konfiguriert. Dabei wurde das Verhalten der Zusatzfunktionalitäten einzeln und allenfalls im Zusammenspiel mit anderen Zusatzfunktionalitäten soweit als möglich analysiert. Die daraus resultierenden Erkenntnisse (inkl. Konfigurationsprobleme und sicherheitsrelevante Aspekte) flossen in diese Arbeit ein. Nach den Einzeltests der Firewalls wurde auch deren Interoperabilität bezüglich VPN untersucht (einige Konfigurationsanleitungen zu diesem Thema befinden sich im Anhang). Eine abschliessende Gegenüberstellung der analysierten Zusatzfunktionalitäten rundet die vorliegende Arbeit ab.

1.5 Verwendete Symbolik

In Kapitel 2 werden mögliche Firewall-Zusatzfunktionalitäten generisch und produktunabhängig beschrieben. Bei jeder Zusatzfunktionalität wird kurz dargelegt, ob es aus Sicht des Autors überhaupt sinnvoll ist, diese auf einer Firewall zu implementieren. Dabei werden folgende Symbole verwendet:

Symbol	*Erläuterungen*
	Die Integration dieser Zusatzfunktionalität direkt auf der Firewall wird als sinnvoll erachtet (um die Bedürfnisse des Betreibers/Administrators der Firewall abdecken zu können; diese Bedürfnisse stehen jedoch unter Umständen im Widerspruch zu den Interessen der Endbenutzer).
	Die Integration dieser Zusatzfunktionalität direkt auf der Firewall erscheint nicht als besonders sinnvoll.

Tabelle 1: Verwendete Symbole zur Beurteilung, ob eine Zusatzfunktionalität sinnvoll erscheint

Ab Kapitel 5 wird bei jeder analysierten Zusatzfunktionalität jeweils am Ende der Beschreibung und Analyse der Zusatzfunktionalität ein Fazit bezüglich Anwendbarkeit und Nutzen der Zusatzfunktionalität und die Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und des sich dahinter befindenden Netzwerks gezogen. Dabei finden folgende Symbole Verwendung:

Symbol	*Erläuterungen*
	➢ **Anwendbarkeit und Nutzen:** Die Anwendbarkeit und/oder der Nutzen der Zusatzfunktionalität können überzeugen ➢ **Gesamtsicherheit:** Die Gesamtsicherheit der Firewall und des internen Netzwerks (LAN) hinter der Firewall wird durch diese Zusatzfunktionalität erhöht
 oder **-**	➢ **Anwendbarkeit und Nutzen:** Die Anwendbarkeit und/oder der Nutzen der Zusatzfunktionalität können nur bedingt überzeugen (Darstellung mit Smiley) ➢ **Gesamtsicherheit:** Die Gesamtsicherheit der Firewall und des internen Netzwerks (LAN) hinter der Firewall wird durch diese Zusatzfunktionalität weder erhöht noch verschlechtert; bezüglich Gesamtsicherheit der zu schützenden Systeme verhält sich die Zusatzfunktionalität indifferent (Darstellung mit **-**)
	➢ **Anwendbarkeit und Nutzen:** Die Anwendbarkeit und/oder der Nutzen der Zusatzfunktionalität können nicht überzeugen ➢ **Gesamtsicherheit:** Die Gesamtsicherheit der Firewall und des internen Netzwerks (LAN) hinter der Firewall wird durch diese Zusatzfunktionalität je nach Konstellation negativ beeinflusst
	Punkte/Eigenschaften, welche die Beurteilung positiv beeinflusst haben
	Punkte/Eigenschaften, welche die Beurteilung negativ beeinflusst haben

Tabelle 2: Verwendete Symbole beim Fazit zu den einzelnen Zusatzfunktionalitäten

Bei einigen Zusatzfunktionalitäten werden sehr detaillierte Tests unter verschiedenen Bedingungen durchgeführt. Folgende Symbole werden zur Visualisierung der entsprechenden Teilresultate eingesetzt:

Symbol	***Erläuterungen***
✓	Das Resultat der durchgeführten Tests entspricht den Erwartungen. Die Zusatzfunktionalität scheint in diesem Bereich wirksam zu sein.
✘	Das Resultat der durchgeführten Tests entspricht nicht den Erwartungen. Die Zusatzfunktionalität scheint in diesem Bereich nicht oder zumindest nicht umfassend wirksam zu sein.

Tabelle 3: Verwendete Symbole bei den Teilresultaten von Zusatzfunktionalitäten-Tests

2. MÖGLICHE ZUSATZFUNKTIONALITÄTEN VON FIREWALLS

Immer mehr Hersteller von Firewalls gehen dazu über, ihre Produkte neben der reinen Grundfunktionalität einer Firewall mit zusätzlichen Eigenschaften auszustatten. Nachfolgend werden mögliche zusätzliche Funktionen einer Firewall beschrieben. Die Aufzählung ist gewiss nicht abschliessend. Jedoch sind zum Teil sicher auch Zusatzfunktionalitäten erwähnt, welche heutzutage in dieser Art und Weise (noch) nicht in allen Firewalls implementiert sind.

Ob es sinnvoll ist, eine Zusatzfunktionalität direkt auf der Firewall zu implementieren, ist sicher auch Ansichtssache. Der Autor hält aufgrund seiner Erfahrung für jede erwähnte mögliche Zusatzfunktionalität fest, ob er eine Integration dieser Funktion direkt auf der Firewall als sinnvoll erachtet oder nicht. Grundsätzlich erscheinen Zusatzfunktionalitäten, welche die Gesamtsicherheit der Firewall oder der sich dahinter befindenden internen Netzwerke verbessern, als sinnvolle Ergänzung einer Firewall, da eine Firewall ja primär eine „Sicherheitsleistung“ erbringen soll. Manche Firewall-Anbieter ziehen es auch vor, anstatt einige der Zusatzfunktionalitäten selber in die Firewall zu integrieren, Schnittstellen zu spezialisierten Tools anzubieten, welche diese Zusatzfunktionalitäten abdecken können. Demgegenüber haben Zusatzfunktionalitäten, welche die Sicherheit der Firewall oder der internen Netzwerke gefährden, auf einer Firewall grundsätzlich nichts zu suchen, da sie in Widerspruch zum Grundgedanken einer Firewall stehen. Neben diesen beiden Gruppen gibt es auch noch Zusatzfunktionalitäten, welche die Sicherheit der Firewall weder verbessern noch verschlechtern, jedoch Bedürfnisse gewisser Betreiberkreise abdecken können.

2.1 Authentisierungsmöglichkeiten

Die Benutzer müssen sich auf der Firewall oder über einen mit der Firewall verbundenen Authentisierserver anmelden (authentisieren), bevor sie gewisse Aktivitäten durchführen können (Autorisierung). Der Firewall-Administrator der Firewall kann dabei definieren, welche Benutzer für welche Aktivitäten entsprechende Berechtigungen erhalten. Dabei kann es sich z.B. um Zugriffsberechtigungen vom externen Netzwerk (WAN) ins interne Netzwerk (LAN) oder vom internen Netzwerk ins externe Netzwerk (z.B. Internetzugang) oder aber um Zugriffsberechtigungen direkt auf die Firewall handeln. Ein autorisierter Benutzer erhält zum Beispiel erst dann Zugriff auf das Internet, nachdem er sich erfolgreich an der Firewall authentisiert hat.

Da die Firewall normalerweise der zentrale Knoten beim Netzübergang vom internen Netzwerk ins externe Netzwerk darstellt, kann mittels Authentisierung besser kontrolliert werden, welche Personen welche Tätigkeiten auf oder durch die Firewall hindurch durchführen.

2.2 Zeiteinschränkung einzelner Firewall-Regeln

Die Firewall lässt zu, dass den einzelnen Regeln ein Zeitintervall zugeordnet werden kann, um festzulegen, wann die Regel zur Anwendung kommt. Eine mögliche Einschränkung ist zum Beispiel, dass bestimmte Regeln jeweils nur während den Bürozeiten oder während der Nacht aktiv sind.

Durch die höhere Granularität der Regelvergabe können die betrieblichen und sicherheitstechnischen Bedürfnisse besser aufeinander abgestimmt werden.

2.3 URL-Filtering, URL-Blocking

Die verschiedenen Firewall-Hersteller verstehen unter diesem Begriff zum Teil unterschiedliche Dinge. Im Rahmen der Diplomarbeit ist mit dieser Funktionalität gemeint, dass die Firewall den Zugriff auf gewisse Web-Seiten aufgrund der URL bzw. ihrer Webadresse unterbindet (Zugriffsschutz vom internen Netzwerk auf das öffentliche Netzwerk, d.h. Einschränkung des Surfverhaltens der Angestellten). Im Idealfall lässt sich diese Einschränkung pro Benutzer und/oder Benutzergruppe definieren. Ausserdem sollte die Firewall die Fähigkeit besitzen, nicht nur URLs in Form von Domänennamen, sondern auch die zugehörigen IP-Adressen korrekt zu blocken.

Da der ganze Netzwerkverkehr vom LAN ins WAN und umgekehrt durch die Firewall läuft, werden unerwünschte Zugriffe auf Internetseiten idealerweise direkt auf der Firewall oder auf einem System mit direkter Anbindung an die Firewall geblockt.

2.4 Content-Filtering

Auch unter diesem Begriff verstehen die verschiedenen Firewall-Hersteller zum Teil unterschiedliche Dinge. Im Rahmen dieser Diplomarbeit ist mit dieser Funktionalität gemeint, dass die Firewall den Zugriff auf gewisse Web-Seiten aufgrund des Web-Seiten-Inhalts oder zumindest auf gewisse Objekte innerhalb der Web-Seite (z.B. gefährliche Java- oder ActiveX-Komponenten) unterbindet (wiederum Zugriffsschutz vom internen Netzwerk auf das öffentliche Netzwerk). Im Idealfall lässt sich diese Einschränkung auch hier pro Benutzer und/oder Benutzergruppe definieren.

Da der ganze Netzwerkverkehr vom LAN ins WAN und umgekehrt durch die Firewall läuft, werden potentiell gefährliche und unerwünschte Inhalte von Webseiten idealerweise auf der Firewall oder auf einem System mit direkter Anbindung an die Firewall gefiltert.

2.5 Virenprüfung

Der Netzwerkverkehr, insbesondere übermittelte Dateien und E-Mail-Attachments, wird auf Viren überprüft. Dies geschieht entweder direkt auf der Firewall oder aber über eine definierte Schnittstelle zu einem kompatiblen Produkt eines Drittherstellers. Infizierte Datenpakete werden verworfen und gelangen nicht ins interne Netzwerk.

Eine Virenprüfung erfolgt normalerweise über mehrere Ebenen und wird auf verschiedenen Systemen wahrgenommen. Auf Viren spezialisierte Firmen mit ihren Anti-Virenlösungen erscheinen für ein umfassendes und effektives Anti-Virenkonzept der bessere Ansatz zu sein als proprietäre Anti-Virenlösungen direkt auf der Firewall.

2.6 SMTP-Filtering

Die Firewall stellt für das SMTP-Protokoll eine Art Applikations-Gateway zur Verfügung. Die Firewall hat dadurch die Möglichkeit, den SMTP-Verkehr zu analysieren und potentiell gefährlichen Inhalt zu verwerfen. Ausserdem lässt sich auf diese Weise die SMTP-Funktionalität gezielt einschränken, indem die Firewall nur eine Teilmenge der möglichen SMTP-Kommandos zum Mail-Server passieren lässt.

Eine solche Funktionalität trägt zu einem höheren Schutz der Systeme hinter der Firewall bei. Da der Verkehr vom WAN in die DMZ oder ins LAN sowieso die Firewall passiert, kann das entsprechende Filtering auch direkt auf der Firewall vorgenommen werden.

2.7 Spam-Filtering

So genannte Spam-Mails werden durch die Firewall geblockt. Bei Spam handelt es sich um Mail-Nachrichten, welche massenweise an beliebige Empfänger gesendet werden, von diesen jedoch nicht angefordert wurden. Auf der Firewall lassen sich bekannte Spam-Absenderadressen oder Stichwörter, welche in den Betreffzeilen von Spam-Mails vorkommen, definieren. E-Mails, welche den auf diese Weise erfassten Kriterien entsprechend, werden von der Firewall verworfen.

Sollte eher in Kombination mit einer dedizierten Anti-Virenlösung implementiert werden, welche eine Schnittstelle zur Firewall aufweist.

2.8 „Intrusion Detection“-Funktionen

Die Firewall verfügt über IDS-Funktionalitäten (IDS steht für Intrusion Detection System). Sie erkennt gewisse Angriffsmuster potentieller Eindringlinge und DoS-Attacken (Denial of Service) und kann entsprechend darauf reagieren. Die Reaktion kann passiver oder aktiver Natur sein. Bei einer passiven Reaktion wird z.B. der Firewall-Administrator alarmiert; bei einer aktiven Reaktion kann die Firewall z.B. eine Regeländerung durchführen und den potentiellen Angreifer für eine gewisse Zeit blocken oder die Verbindung zum potentiellen Angreifer abbrechen.

Die Erkennung der am häufigsten auftretenden Eindringungsversuche direkt durch die Firewall stellt sicher eine sinnvolle Ergänzung zu den Grundfunktionalitäten dar. Umfassende „Intrusion Detection“-Lösungen erfordern jedoch mehrere Sensoren, welche im Netzwerk verteilt sind. Eine reine Firewall-Lösung greift deshalb zu kurz.

2.9 Anti-Spoofing (IP-Spoofing)

Die Firewall soll verhindern, dass gefälschte IP-Quell-Adressen entweder vom öffentlichen Netz ins interne Netz oder vom internen Netz ins öffentliche Netz gelangen. Die Firewall muss somit wissen, welche IP-Adressen auf welchem Interface Gültigkeit haben. Das exter-

ne Interface der Firewall darf deshalb keine Pakete mit IP-Quell-Adressen des internen Netzwerks und das interne Interface sollte demgegenüber nur Pakete mit IP-Quell-Adressen des internen Netzes akzeptieren.

👍 Die Firewall hat Kenntnis davon, welche IP-Adressen im normalen Netzwerkverkehr auf welchem Interface zu erwarten sind und kann allfällige Abweichungen deshalb unmittelbar und zeitgerecht feststellen.

2.10 Überwachung der Internetaktivitäten

Die Firewall kann das Surfverhalten der einzelnen Internetbenutzer überwachen und statistisch auswerten. Es kann festgestellt werden, wer wie lange auf welchen Internetseiten aktiv war. Auf diese Weise können zudem Aussagen bezüglich Ressourcenbedarf (z.B. benötigter Datendurchsatz) gemacht werden.

👍 Aus Sicht des Betreibers (des Unternehmens) durchaus sinnvoll. Spezialisierte Softwarepakete von Drittherstellern auf dedizierten Systemen können diese Funktion jedoch unter Umständen besser abdecken.

2.11 Erweiterte Logging-Möglichkeiten

Die durch die Firewall erstellte Log-Datei enthält neben den rudimentären Angaben weiterführende Hinweise, wie z.B. Häufigkeit des Auftretens eines bestimmten Eintrags, möglich Ursachen, Angaben zu möglichen Angriffen durch Hacker, allenfalls getroffene Gegenmassnahmen usw. Die Log-Dateien lassen sich nach beliebigen Kriterien sortieren und/oder filtern und in der Log-Datei kann nach Einträgen gesucht werden. Berichte und Statistiken zu den Log-Einträgen können erstellt und die Resultate grafisch aufbereitet werden. Ausserdem lässt sich die Log-Datei an einen zentralen Log-Server (z.B. Syslog-Server) zur Auswertung senden.

👍 Dabei handelt es sich um eine gezielte Erweiterung der Firewall-Grundfunktionalität „Logging“.

2.12 Alarmierung

Der Firewall-Administrator kann festlegen, unter welchen Umständen (z.B. bei gewissen Regel-Verletzungen) ein Alarm ausgelöst werden soll. Ausserdem kann definiert werden, wie der Alarm in Erscheinung treten soll (z.B. als Konsolen-Meldung auf dem Bildschirm der Firewall-Managementstation, als E-Mail, als Pager- oder als SMS-Meldung an den Administrator).

👍 Stellt eine Erweiterung der Grundfunktionalität „Logging“ dar.

2.13 Unterstützung von NAT und/oder PAT

Die Firewall unterstützt die Konzepte von NAT (Network Address Translation) und/oder PAT (Port Address Translation). Mit Hilfe von NAT kann einerseits die Anzahl der benötigten öffentlichen IP-Adressen klein gehalten werden und andererseits bietet NAT einen gewissen Schutz der internen Systeme, da diese je nach NAT-Konfiguration nicht direkt aus dem öffentlichen Netzwerk erreichbar respektive sichtbar sind.

Je nach Produkthersteller werden diese Begriffe unterschiedlich verwendet. Bei NAT kann grundsätzlich zwischen zwei Hauptvarianten unterschieden werden:

Dynamisches NAT — Mehreren internen (meist privaten) IP-Adressen wird beim Netzübergang durch die Firewall eine andere (meist öffentliche) IP-Adresse zugeordnet (alle internen Systeme erhalten die gleiche öffentliche IP-Adresse); es besteht somit eine „N:1-Beziehung“. Der Firewall-Hersteller Check Point nennt diese Art von NAT „Hide Mode NAT“ oder heutzutage auch „Dynamic Mode NAT“ und der Firewall-Hersteller Cisco bezeichnet diesen Vorgang als PAT.

Statisches NAT — Einer internen (meist privaten) IP-Adresse wird beim Netzübergang durch die Firewall eine andere (meist öffentliche) IP-Adresse zugeordnet (jedes interne System erhält eine eigene öffentliche IP-Adresse); es besteht somit eine „1:1-Beziehung“. Der Firewall-Hersteller Check Point nennt diese Art von NAT „Static Mode NAT“ und der Firewall-Hersteller Cisco bezeichnet diesen Vorgang einfach als NAT.

In der vorliegenden Arbeit werden die beiden Begriffe dynamisches und statisches NAT verwendet.

NAT ist heutzutage nicht mehr aus der Netzwerklandschaft wegzudenken. Nur eine Firewall, welche dieses Konzept unterstützt, lässt sich effektiv am Perimeter zwischen dem internen und dem öffentlichen Netzwerk einsetzen.

2.14 DHCP-Server

Die Firewall verfügt über einen eigenen DHCP-Server, welcher den Clients automatisch eine freie IP-Adresse und die IP-Adressen der DNS-Server zuteilen kann.

Vor allem in kleineren Netzwerken, welche über keinen dedizierten DHCP-Server verfügen, eine sinnvolle Ergänzung.

2.15 Zeitserver-Dienst

Die Firewall kann ihre Systemzeit von einem Zeitserver im eigenen Netzwerk oder von einem Zeitserver im Internet beziehen. Mit einem Zeitserver wird sichergestellt, dass die zentralen Systeme (insbesondere die Firewall und die Server) alle über die gleiche Systemzeit verfügen. Eine einheitliche und korrekte Systemzeit (auch auf der Firewall) kann im Fall von Prob-

lemen oder eines Hackingangriffs elementar wichtig sein, um den zeitlichen Ablauf des Vorfalls rekonstruieren und nachvollziehen zu können.

Es kann sichergestellt werden, dass die Firewall über die gleiche Systemzeit wie die übrigen (Server-)Systeme verfügt.

2.16 Dynamisches DNS

Mittels dynamischem DNS besteht die Möglichkeit, einer sich von Zeit zu Zeit ändernden IP-Adresse einen fixen DNS-Namen zuzuordnen. Diese Dienstleistung wird mittlerweile von mehreren Unternehmen oder Organisationen angeboten. Eine Liste solcher Anbieter kann z.B. unter http://www.technopagan.org/dynamic gefunden werden. Eine solche Dienstleistung ist vor allem für Benutzer interessant, welche über keine eigenen öffentlichen IP-Adressen verfügen und die öffentliche IP-Adresse jeweils dynamisch durch ihren Internet Service Provider (ISP) zugeteilt erhalten. Falls solche Benutzer, auch ohne eigene öffentliche IP-Adresse, Dienste (z.B. Zugriff auf den eigenen Web-Server) im Internet anbieten wollen, sehen sie sich vor dem Problem, dass sie die jeweils gültige dynamische IP-Adresse mitteilen müssen, damit überhaupt auf ihr Angebot zugegriffen werden kann. Die Lösung für dieses Problem liefern die Anbieter von dynamischen DNS-Diensten. Der Benutzer muss lediglich seine jeweils gültige IP-Adresse, welche er dynamisch durch seinen ISP erhalten hat, dem dynamischen DNS-Dienst mitteilen. Auf diese Weise ist er immer unter dem gleichen DNS-Namen im Internet erreichbar, auch wenn seine IP-Adresse ständig ändert. Die Mitteilung der jeweils aktuellen IP-Adresse sollte natürlich möglichst zeitgerecht erfolgen. Dazu sind diverse Programme erhältlich, welche diese Aufgabe automatisiert übernehmen. Mittlerweile haben auch viele Hersteller von ADSL-Routern und Firewalls den Nutzen dieser Dienstleistung erkannt und den dynamischen DNS-Update-Dienst direkt in ihre Produkte integriert.

Da eine Firewall oft, neben einem allfälligen zusätzlichen Router, den Netzwerkübergang ins Internet darstellt, macht die Integration dieser Funktion auf der Firewall durchaus Sinn. Je nachdem kann sie jedoch auch auf dem äussersten Router (Border Router) beim Netzübergang ins Internet angeboten werden.

2.17 Wireless-LAN (WLAN)

In der Firewall ist ein WLAN-Accesspoint integriert. Dadurch wird den WLAN-Clients die Möglichkeit gegeben, über die Firewall auf das Internet zuzugreifen und/oder eine Verbindung mit den „kabelgebundenen“ Systemen des internen Netzwerkes aufzubauen. Da die Wireless-Technologie zum heutigen Zeitpunkt nach wie vor einige, zum Teil schwerwiegende, Sicherheitsmängel aufweist, ist bei einer Integration dieser Funktionalität auf einer Firewall besondere Vorsicht angebracht.

Aufgrund der mit dieser Technologie verbundenen inhärenten Risiken erscheint die Implementation dieser Zusatzfunktionalität direkt auf der Firewall als zu riskant. Falls effektiv WLANs zum Einsatz kommen sollen, stellt die Platzierung des Accesspoints ausserhalb der Firewall sicherlich die bessere Variante dar.

2.18 Virtual Private Network (VPN)

Die Firewall dient als Endpunkt einer VPN-Verbindung und unterstützt den IPSec-Standard (Internet Protocol Security). Dadurch ist es möglich, Daten verschlüsselt über ein unsicheres öffentliches Netzwerk (z.B. Internet) zu transferieren. Auf diese Weise kann die Vertraulichkeit und Integrität der Daten gewährleistet werden. Vorteile einer VPN-Implementation direkt auf der Firewall sind, dass alle Benutzer des internen Netzwerks transparent von der VPN-Funktionalität Gebrauch machen können und dass keine Installation von Zusatzprodukten (Hard- oder Software) auf Clientseite nötig ist; allerdings werden dabei die Daten im internen Netzwerk nach wie vor unverschlüsselt übertragen.

Eine gesicherte und vertrauliche End-to-End-Verbindung zwischen Partnern über das öffentliche unsichere Internet stellt heutzutage eine kostengünstige und betriebswirtschaftlich interessante Alternative zu Stand- und Mietleitungen dar. Bei VPN handelt es sich deshalb um eine der wichtigsten Zusatzfunktionalitäten, welche eine Firewall bieten kann.

2.19 Diagnose-Tools

Der Firewall-Hersteller stellt Diagnose-Tools zur Verfügung, damit beim Auftreten von Störungen an der Firewall der Firewall-Administrator entsprechende Untersuchungen durchführen kann.

Im Fall von Störungen lässt sich das Problem auf diese Weise einfacher eruieren und die Verfügbarkeit der Firewall kann dadurch erhöht werden.

2.20 Remote-Management

Dem Firewall-Administrator wird die Möglichkeit geboten, neben der Konfiguration und des Managements der Firewall direkt an der Konsole, diese auch aus der Ferne über das Netzwerk zu verwalten. Dabei können verschiedene Protokolle, wie z.B. HTTP, Telnet, FTP, SNMP, SSH, SSL usw.) zum Einsatz kommen. Es gibt auch Firewalls, welche nur noch auf diese Weise konfiguriert werden können und ein direkter Konsolenzugang gar nicht zur Verfügung steht. Grundsätzlich stellt sich bei einer Firewall-Konfiguration über das Netzwerk die Frage, ob der entsprechende Netzwerkverkehr mittels Verschlüsselung abgesichert werden kann.

Die Möglichkeit, sicheres Remote-Management der Netzwerkkomponenten und der Serversysteme durchführen zu können, trägt wesentlich zum effizienten Einsatz und Unterhalt der Systeme bei. Ohne diese Möglichkeit müssten die Geräte ausschliesslich über die Konsole administriert werden, was in grösseren Netzwerken sehr umständlich und ineffizient wäre.

2.21 Firmware- bzw. Firewall-Updates

Der Firewall-Administrator kann die Firmware (Betriebssystem einer integrierten Firewall, welche aus Hard- und Software besteht, wie z.B. ZyXEL ZyWALL) oder die Firewall-Software (bei softwarebasierten Firewalls, wie z.B. Check Point Firewall-1) selbständig aktualisieren. Auch Firewalls sind oft vor Sicherheitslücken nicht gefeit, deshalb ist es wichtig, dass die Hersteller allenfalls vorhandene Sicherheitslücken ihrer Produkte beheben und die Fehlerkorrekturen in Form von neuer Firmware oder von Sicherheits-Patches für die Firewall-Software den Firewall-Administratoren zur Verfügung stellen. Ein Update der neuen Firmware oder der Firewall-Software sollte möglichst unkompliziert durchgeführt werden können.

👍 Unentbehrlich, um die Sicherheit der Firewall über die Zeitdauer hinweg auf einem hohen Niveau halten zu können.

2.22 Dial-Up-Backup, Verkehrsumleitung

Die Firewall (vor allem integrierte Firewalls bestehend aus Hard- und Software) kann auf eine Wählleitung ausweichen, falls der primäre Zugang zum Internet/WAN nicht verfügbar ist. Die Firewall prüft, ob ein definiertes Zielsystem im WAN angesprochen werden kann. Falls dies nicht der Fall ist, stellt die Firewall automatisch eine Verbindung über eine Backup-Wählleitung (analog oder ISDN) und einen anderen ISP her. Sobald das Zielsystem im WAN wieder über das primäre Interface erreichbar ist, wird die Backup-Verbindung abgebaut und der Verkehr fliesst wieder über die ursprüngliche WAN-Verbindung.

👍 Erhöht die Gesamtverfügbarkeit der Firewall.

2.23 Backup und Restore der Firewall-Konfiguration

Die Konfiguration der Firewall (inkl. die Konfiguration der Zusatzfunktionalitäten) lässt sich einfach und effektiv sichern, um diese im Falle einer Störung (z.B. Hardwareausfall) oder bei durchgeführten Fehlkonfigurationen zeitgerecht wiederherstellen zu können.

👍 Nur wenn ein Backup bzw. Restore der Firewall-Konfiguration möglich ist, kann diese im Falle von Problemen ohne grossen Zeitverlust wiederhergestellt werden.

2.24 Hohe Verfügbarkeit

Die Firewall kann mit einer zweiten Firewall des gleichen Typs parallel geschaltet werden. Die eine Firewall ist aktiv, die andere befindet sich im Hot-Standby-Modus. Sobald die aktive Firewall den Dienst aufgrund von Problemen nicht mehr verrichten kann, übernimmt die andere Firewall deren Funktion nahtlos. Dazu besteht unter den beiden Firewalls eine dedizierte Verbindung, über welche die Status-Informationen ausgetauscht werden.

👍 Erhöht die Gesamtverfügbarkeit der Firewall-Infrastruktur.

2.25 Lastverteilung / Load Balancing

Die Firewall kann mit einer zweiten oder mehreren Firewalls des gleichen Typs parallel betrieben werden, wobei jedoch alle Firewalls aktiv sind. Der anfallende Netzwerkverkehr fliesst somit durch irgendeine der aktiven Firewalls; es findet eine Lastverteilung des Netzwerkverkehrs über alle Firewalls hinweg statt. Falls eine der Firewalls ausfällt, übernehmen die anderen Firewalls einfach den ganzen Netzwerkverkehr.

Erhöht die Gesamtverfügbarkeit der Firewall-Infrastruktur.

3. SELEKTIONSKRITERIEN FÜR DIE ZU ANALYSIERENDEN FIREWALLS

Die im Rahmen dieser Diplomarbeit analysierten Firewalls wurden aufgrund der folgenden Kriterien ausgewählt:

- Berücksichtigung von Firewalls, welche in der Praxis häufig anzutreffen sind, also möglichst keine exotischen Produkte
- Zusammenstellung eines „ausgewogenen" Produktportfolios mit Firewalls, welche in KMUs anzutreffen sind und mit Firewalls, welche eher in grösseren Unternehmen zum Einsatz kommen
- Berücksichtigung von Firewalls, welche über möglichst viele Zusatzfunktionalitäten verfügen

Aufgrund dieser Kriterien wurden verschiedene Produkte vorselektiert und evaluiert, bis schliesslich die folgenden Produkte ausgewählt wurden:

- ZyXEL ZyWALL 10W
- SonicWALL SOHO3 25-User mit VPN
- Check Point Firewall-1 Next Generation (NG) Feature Pack (FP) 3

4. ÜBERSICHT ÜBER DIE FUNKTIONALITÄTEN DER ANALYSIERTEN FIREWALLS

Dieses Kapitel liefert einen kurzen Überblick über die gemäss Produkteinformationen und Handbüchern der jeweiligen Firewall-Hersteller angepriesenen (Zusatz-)Funktionalitäten resp. Eigenschaften der in der vorliegenden Diplomarbeit analysierten Firewalls. Die Beurteilung und die Testresultate bezüglich dieser Zusatzfunktionalitäten sind in den darauf folgenden Kaptiteln zu finden.

4.1 ZyXEL ZyWALL 10W

Die ZyXEL ZyWALL 10W verfügt gemäss Produktprospekt und Handbuch insbesondere über folgende Eigenschaften:

Eigenschaft	***Nähere Erläuterungen***
Firewall-Sicherheit	➢ Paket-Filter ➢ Stateful Inspection ➢ Denial of Service (DOS) Erkennung ➢ Angriffsalarmierung und Logdateien ➢ Zugriffskontrolle
Virtual Private Network (VPN)	➢ 10 parallele IPSec-Verbindungen
Routing-Unterstützung	➢ IP-Routing basierend auf TCP, UDP, ICMP, ARP, RIP V1 & RIP V2 ➢ Programmierbare statische Routen ➢ IP-Alias-Adressen können vergeben werden
Inhaltsfilterung (Content-Filtering und URL-Filtering)	➢ Java, ActiveX, Cookies, Web-Proxies ➢ URL-Filtering
ISP-Authentisierung	➢ PPPoE (Point-to-Point over Ethernet) ➢ PPTP (Point-to-Point Tunneling Protocol)
Netzwerk-Management	➢ Web-basierende Konfiguration ➢ Telnet Remote Access Unterstützung ➢ TFTP/FTP für Firmware-Update / -Backup ➢ SNMP-Unterstützung
Applikationen	➢ DHCP-Server ➢ DNS-Proxy ➢ Internet Zeitserver-Dienst ➢ Verkehrs-Umleitung ➢ Dynamisches DNS ➢ Telnet-Client

	➢ Eingebaute Diagnose-Werkzeuge ➢ Universal Plug and Play (UPnP) ➢ Dial-Up-Backup (Modemanschluss direkt an der Firewall)
Wireless-LAN (WLAN)	➢ IEEE 802.11b kompatibel ➢ IPSec über WLAN ➢ 64/128-Bit WEP-Verschlüsselung ➢ IEEE 802.1x anschlussbasierende Authentisierung mit RADIUS-Client

Tabelle 4: ZyWALL 10W – Eigenschaften

4.2 SonicWALL SOHO3 25-User mit VPN

Gemäss Produktprospekt und Handbuch verfügt die SonicWALL SOHO3 unter anderem über folgende Eigenschaften:

Eigenschaft	***Nähere Erläuterungen***
Internet-Verbindung	➢ Mit der vorhandenen Lizenz können bis zu 25 Benutzer (IP-Adressen des internen Netzwerks) gleichzeitig auf das Internet zugreifen
Firewall-Sicherheit	➢ Stateful Inspection ➢ Denial of Service (DoS) Erkennung ➢ Angriffsalarmierung und Logdateien ➢ Zugriffskontrolle
Virtual Private Network (VPN)	➢ 10 parallele IPSec-Verbindungen ➢ VPN mit Hardware-Beschleunigung (dedizierter ASIC-Chip ⇨ Application-Specific Integrated Circuit)
Routing-Unterstützung	➢ IP-Routing basierend auf TCP, UDP, ICMP, ARP ➢ Programmierbare statische Routen ➢ IP-Alias-Adressen können vergeben werden
Inhaltsfilterung (Content-Filtering und URL-Filtering)	➢ Java, ActiveX, Cookies, Web-Proxies, bekannte gefälschte digitale Zertifikate ➢ URL-Filtering
ISP-Authentisierung	➢ PPPoE (Point-to-Point over Ethernet) ➢ PPTP (Point-to-Point Tunneling Protocol) ➢ L2TP (Layer 2 Tunneling Protocol)
Netzwerk-Management	➢ Web-basierende Konfiguration mittels HTTP oder HTTPS ➢ SNMP-Unterstützung

Applikationen	➢ Anti-Viren-Schutz übers Internet in Zusammenarbeit mit McAfee ➢ DHCP-Server ➢ Web-Proxy-Forwarding ➢ Internet Zeitserver-Dienst ➢ Eingebaute Diagnose-Werkzeuge

Tabelle 5: SonicWALL SOHO3 – Eigenschaften

4.3 Check Point Firewall-1 Next Generation (NG)

Von Check Point sind zahlreiche Teilmodule zur Firewall erhältlich. Einige der Kerneigenschaften der Firewall sind (Aufzählung nicht abschliessend):

Eigenschaft	***Nähere Erläuterungen***
Firewall-Sicherheit	➢ Stateful Inspection ➢ Denial of Service (DoS) Erkennung ➢ Angriffsalarmierung und Logdateien ➢ Zugriffskontrolle mittels Benutzerauthentisierung
Virtual Private Network (VPN)	➢ VPN-Verbindungen sowohl für Extranets als auch für Remote Access Benutzer
Inhaltsfilterung (Content-Filtering und URL-Filtering)	➢ Content-Filtering teilweise in der Firewall integriert ➢ Erweitertes Content-Filtering und URL-Filtering durch Anbindung von Drittprodukten
Netzwerk-Management	➢ Eigene Firewall-Management-Clients mit grafischer Oberfläche ➢ Verschlüsselte Kommunikation zwischen den verschiedenen Firewall-Modulen ➢ SNMP-Unterstützung
Update / Unterhalt der Firewall-Produkte	➢ Zentrale Verwaltung der Firewall-Lizenzen und automatisierte Updates der einzelnen Firewall-Module
Erweiterungen / Modularität	➢ OPSEC (Open Platform for Security) Schnittstelle

Tabelle 6: Check Point Firewall-1 NG – Eigenschaften

5. ZyXEL ZyWALL 10W

5.1 Allgemeine Hinweise zur Firewall

Bei dieser Firewall handelt es sich um ein Produkt, welches auf den KMU-Markt (so genannter SOHO-Markt; SOHO steht für Small Office / Home Office) abzielt. Innerhalb der ZyXEL-Firewall-Produktfamilie ist das Modell ZyWALL 10W ungefähr in der Mitte anzusiedeln[3].

Die Firewall arbeitet nach dem „Stateful Inspection"-Prinzip, d.h. sie führt in einer Zustandstabelle die aktuellen Verbindungen und kann, vereinfacht gesagt, unter anderem aufgrund dieser Zustandstabelle entscheiden, welcher Verkehr aus dem WAN in das LAN zugelassen werden soll. Die Firewall verfügt über zwei Interface – ein internes Interface und ein externes Interface; ein so genannter DMZ-Port (drittes Interface) ist nicht vorhanden. Auf der Firewall können maximal 50 Firewall-Regeln definiert werden und die Log-Datei nimmt maximal 128 Einträge auf.

Die Firewall kann sowohl „lokal" über den Consolen-Port, als auch „remote" über die Protokolle HTTP, Telnet und FTP administriert werden.

Die während dieser Diplomarbeit gewonnen Erkenntnisse zu den Zusatzfunktionalitäten der ZyWALL 10W Firewall basieren alle auf der zu diesem Zeitpunkt aktuellen Firmware 3.60(wh2).

Zum Testen der Firewall-Zusatzfunktionalitäten wurde folgende Versuchsumgebung aufgebaut:

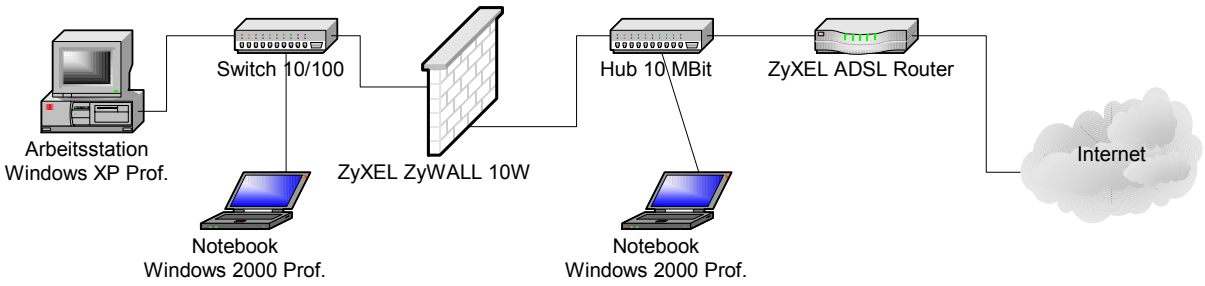


Abbildung 1: ZyWALL 10W – Versuchsumgebung für die Durchführung der Firewall-Tests

Die Windows XP Arbeitsstation und das Windows 2000 Notebook waren mit diversen Tools (Portscanner, Sniffer usw.) ausgestattet, um die technischen Tests möglichst umfassend durchführen zu können. Das Notebook konnte wahlweise entweder hinter der Firewall am Switch oder vor der Firewall am Hub angeschlossen werden.

[3] ZyXEL-Firewall-Produkteübersicht, siehe http://www.zyxel.com/product/category.php?indexFlagvalue=1021873683

5.2 Grundkonfiguration und wesentliche Standardeinstellungen

Die Konfiguration der Firewall kann über den an der Firewall vorhandenen Konsolen-Port oder aber mittels Remote-Management über die Protokolle HTTP oder Telnet erfolgen. Das interne Interface der Firewall ist standardmässig auf die IP-Adresse 192.168.1.1 konfiguriert und das Initialpasswort lautet „1234“. Beim erstmaligen Management-Zugriff auf die Firewall mittels HTTP wird der Administrator aufgefordert, das Initialpasswort zu ändern. Leider ist es jedoch möglich, diese Aufforderung zu ignorieren (beim nächsten Login mittels HTTP erscheint sie allerdings wieder von neuem) oder das vorhandene Passwort „1234“ einfach durch ein Leer-Passwort, d.h. kein Passwort, zu ersetzen. Interessanterweise ist das Setzen eines Leer-Passwortes beim Management-Zugang über die Konsole oder mittels Telnet nicht möglich, hier muss das Passwort aus mindestens einem Leerzeichen (Space) bestehen. Hingegen erscheint beim erstmaligen Management-Zugriff über die Konsole oder mittels Telnet die Aufforderung für den Passwortwechsel im Unterschied zum HTTP-Zugang nicht!

Nach der ersten Inbetriebnahme weist die Firewall folgende Einstellungen auf:

- Firewall ist aktiviert
- Vom LAN ins LAN (via Firewall) ist aller Verkehr erlaubt (wird nicht geloggt)
- Vom LAN ins WAN ist aller Verkehr erlaubt (wird nicht geloggt)
- Vom WAN ins LAN ist aller Verkehr verboten (wird geblockt und geloggt)
- Vom WAN ins WAN (via Firewall) ist folgender Verkehr erlaubt:
  - Von irgendwoher (any) nach irgendwohin (any) sind die UDP-Ports 68 (Bootp-Client) und 500 (IKE – Internet Key Exchange) erlaubt
  - Der übrige Verkehr ist verboten (wird geblockt und geloggt)
- Schwellenwerte zum Erkennen von DoS-Attacken sind definiert und aktiviert
- Internes Interface:
  - IP-Adresse 192.168.1.1 / 255.255.255.0
  - DHCP-Server aktiv mit IP-Startadresse 192.168.1.33 und einem IP-Adressenpool von 32 Adressen
  - RIP-1 (Routing Information Protocol) in beide Richtungen aktiv (Firewall führt Routing-Table-Broadcasting durch und nimmt RIP-Informationen von anderen Routern entgegen)
- Externes Interface:
  - WAN ISP ist auf den Typ „Ethernet“ eingestellt
  - DHCP-Client ist aktiviert
  - Dynamisches NAT (N:1) für Verkehr aus dem LAN ins WAN
- Remote Management
  - Telnet (TCP-Port 23), alle IP-Adressen LAN und WAN zugelassen
  - FTP (TCP-Port 21), alle IP-Adressen LAN und WAN zugelassen
  - WWW (TCP-Port 80), alle IP-Adressen LAN und WAN zugelassen
  - SNMP (UDP-Port 161), alle IP-Adressen LAN und WAN zugelassen, Standard-Community-Strings „public“ für Lesen (GET) und Schreiben (SET) und Standard-Community-Trap „public“
- Logging ist aktiviert für: System Maintenance, System Errors, Access Control, UPnP, Forward Web Sites, Blocked Web Sites, Blocked Java etc., Attacks, IPSec, IKE

Folgende Funktion konnte während der Testphase nicht erfolgreich konfiguriert werden:

- Wireless-LAN Accesspoint-Benutzerauthentisierung mittels EAP basierend auf dem IEEE 802.1x-Standard

Fazit Grundkonfiguration und wesentliche Standardeinstellungen

Beurteilung der Grundkonfiguration bezüglich Aufwand, Verständlichkeit usw. ☺

Auswirkungen der Grundkonfiguration auf die Gesamtsicherheit der Firewall ☹

⊕

- Aufforderung zum Wechsel des Initialpassworts bei Konfiguration mittels HTTP
- Wesentliche Einstellungen können mit Hilfe eines Konfigurations-Wizards durchgeführt werden
- Konsolen-Port zur Konfiguration vorhanden
- Gesamter Verkehr vom WAN ins LAN wird standardmässig geblockt
- „Intrusion Detection"-Funktionen sind aktiviert
- Logging ist aktiviert

⊖

- Setzen eines Leer-Passwortes (d.h. kein Passwort) bei Konfiguration mittels HTTP möglich
- Keine Aufforderung zum Wechsel des Initialpassworts bei Konfiguration mittels Konsole oder Telnet
- SNMP ist standardmässig aktiv und verfügt über den Standard-Community-String „public"

5.3 Zusatzfunktionalitäten

Die Zusatzfunktionalitäten werden im folgenden Kapitel grundsätzlich in der gleichen Reihenfolge, in der sie in Kapitel 2 generisch umschrieben wurden, abgehandelt. Falls die Firewall eine der in Kapitel 2 erwähnten Zusatzfunktionalitäten nicht unterstützt, wird diese in diesem Kapitel auch nicht aufgeführt (es erfolgt somit kein expliziter Hinweis, dass die entsprechende Funktionalität nicht zur Verfügung steht; eine Gesamtübersicht über alle Zusatzfunktionalitäten folgt in Kapitel 8).

Es gilt zudem zu berücksichtigen, dass die Konfiguration einiger in Kapitel 2 erwähnten Zusatzfunktionalitäten auf der Firewall jeweils an ein und derselben Stelle bzw. im gleichen Menu erfolgt. In einem solchen Fall werden diese Zusatzfunktionalitäten auch im vorliegenden Kapitel entsprechend zusammengefasst.

Am Schluss dieses Kapitels (ab Kapitel 5.3.16) werden noch weitere interessante Eigenschaften der Firewall, welche jedoch in Kapitel 2 keine Berücksichtigung als eigenständige Zusatzfunktionalitäten fanden (es handelt sich dabei mehr um willkommene Eigenschaften als um echte Zusatzfunktionalitäten), in gleicher Art und Weise wie die übrigen Zusatzfunktionalitäten umschrieben.

5.3.1 Content- und URL-Filtering

ZyXEL fasst unter dem Betriff „Content Filtering" sowohl das Content-Filtering, als auch das URL-Filtering/-Blocking zusammen (siehe Kapitel 2.3 und 2.4 bezüglich der Definition dieser Begriffe, wie sie in dieser Arbeit verwendet werden).

Unter dem Begriff „Restrict Web Features" lassen sich auf der Firewall ActiveX-Controls, Java-Applets (ohne JavaScript), Cookies und Web-Proxies filtern. Die nachfolgende Tabelle zeigt die diesbezüglich durchgeführten Tests und deren Ergebnisse auf:

Getestete Funktion	***Durchgeführte Tests***	***Ergebnisse / Erkenntnisse***	
ActiveX-Filter	➢ ActiveX-Filter in der Firewall aktiviert ➢ Konkrete Tests mit ActiveX-Controls auf einer ActiveX-Demo-Website[4] (Websitezugriff mittels HTTP-Protokoll) Verwendeter Browser: Internet Explorer 6.0 ➢ Konkrete Tests mit ActiveX-Controls innerhalb des kostenpflichtigen Sicherheitsportals eSecurityOnline[5] (Reporting-Funktionen, welche auf ActiveX-Controls basieren ⇨ Websitezugriff mittels HTTPS-Protokoll) Verwendeter Browser: Internet Explorer 6.0	Die ActiveX-Controls auf der Demo-Website wurden durch die Firewall erfolgreich geblockt resp. das Herunterladen der Controls wurde verhindert. Das ActiveX-Control von eSecurityOnline konnte trotz aktiviertem ActiveX-Filter in der Firewall heruntergeladen und ausgeführt werden. Dieses Verhalten ist jedoch nachvollziehbar, da der ganze Netzwerkverkehr mittels SSL verschlüsselt wurde und die Firewall das ActiveX-Control deshalb nicht feststellen konnte. Fazit: Der ActiveX-Filter arbeitet grundsätzlich wie erwartet. Sobald der Website-Zugriff mittels SSL-Verschlüsselung erfolgt (HTTPS), können ActiveX-Controls jedoch trotz aktiviertem Filter heruntergeladen und ausgeführt werden.	✓
Java-Filter	➢ Java-Filter in der Firewall aktiviert ➢ Test der Java-Funktion mittels Heise-Browsercheck. Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a ➢ Test der Homepage des Autors[6], auf welcher die Navigationsleiste in Java programmiert wurde (normaler Internet-Zugriff mittels HTTP-Protokoll) Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a ➢ Test der Homepage des Autors auf einem eigenen Test-Server mit einem SSL-Serverzertifikat von Thawte[7] zu Evaluationszwecken (Websitezugriff mittels HTTPS-Protokoll) Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a	Die Java-Applets wurden sowohl auf der Heise-Browsercheck-Seite, als auch auf der Homepage des Autors beim Zugriff mittels HTTP-Protokoll nicht mehr angezeigt. Beim Zugriff mittels HTTPS-Protokoll auf die Homepage des Autors (eigener Testserver) wird das Java-Applet heruntergeladen und ausgeführt. Dieses Verhalten ist jedoch nachvollziehbar, da der ganze Netzwerkverkehr mittels SSL verschlüsselt wurde und die Firewall das Java-Applet deshalb nicht feststellen konnte. Fazit: Java-Applets werden bei den getesteten Browsern grundsätzlich korrekt geblockt. Sobald der Website-Zugriff mittels SSL-Verschlüsselung erfolgt (HTTPS), können die Java-Applets jedoch trotz aktiviertem Filter heruntergeladen und ausgeführt werden.	✓
Cookie-Filter	➢ Cookie-Filter in Firewall aktiviert ➢ Aufruf folgender Homepages mit den Browsern Internet Explorer 5.5 und 6.0 und Mozilla 1.2a und 1.3a: ○ Swiss-Homepage, Login-Seite[8] ○ Amazon-Homepage[9] ○ Homepage des Autors Alle diese Homepages setzten im Normalfall beim Besuch der Homepage ein Cookie auf dem PC des Besuchers	Je nach verwendetem Browser verhält sich der Cookie-Filter unterschiedlich. ***Internet Explorer 5.5 und 6.0*** ➢ Die Swiss-Homepage kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben ➢ Die Amazon-Homepage kann nicht mehr aufgerufen werden und somit wird auch kein Cookie geschrieben ➢ Homepage des Autors kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter	✘

[4] OCX-Tester, siehe http://www.ilook.fsnet.co.uk/vb/vbdemo.htm
[5] eSecurityOnline, siehe http://www.esecurityonline.com
[6] tomsplace, siehe http://www.tomsplace.ch
[7] Thawte, siehe http://www.thawte.com
[8] Swiss-Homepage, siehe http://www.swiss.com/net/index/tg-ob-mp-create-and-change.htm
[9] Amazon-Homepage, siehe http://www.amazon.de

Getestete Funktion	*Durchgeführte Tests*	*Ergebnisse / Erkenntnisse*	
		geschrieben. Das Cookie kann beim nächsten Besuch auch wieder ohne Probleme ausgelesen werden Fazit Internet Explorer: Keine der besuchten Homepages verhält sich wie erwartet. Die Cookies können trotz aktivem Cookie-Filter geschrieben werden und die Amazon-Homepage lässt sich gar nicht mehr aufrufen. Das letztgenannte Verhalten sollte eigentlich trotz aktiviertem Cookie-Filter nicht auftreten. ***Mozilla 1.2a und 1.3a*** ➢ Die Swiss-Homepage kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben ➢ Die Amazon-Homepage kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben ➢ Homepage des Autors kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben. Das Cookie kann beim nächsten Besuch auch wieder ohne Probleme ausgelesen werden Fazit Mozilla: Mit diesem Browser lassen sich zumindest noch alle Homepages aufrufen. Die Cookies werden jedoch trotz aktivem Cookie-Filter auf den Benutzer-PC geschrieben. Gesamtfazit: Der Cookie-Filter arbeitet nicht wie erwartet, die Cookies aller getesteten Webseiten werden trotz aktivem Filter auf den Benutzer-PCs gespeichert und auch wieder ausgelesen (Test mittels Homepage des Autors). Bei den getesteten Webseiten ist deshalb kein Unterschied im Verhalten bezüglich Cookies zwischen aktiviertem und deaktiviertem Cookie-Filter ersichtlich.	
Web-Proxy-Filter	➢ Web-Proxy-Filter in Firewall aktiviert ➢ Internet-Zugriffsversuche mit im Browser aktiven Proxy-Einstellungen eines externen Web-Proxies (Proxy-Server befindet sich im WAN). Tests sowohl mit dem Proxy-Server des eigenen ISPs (Solnet) als auch mit öffentlichen Proxies (zufällige Auswahl)[10] ➢ Internet-Zugriffsversuche mittels lokalem Web-Proxy[11], welcher ebenfalls im Browser als Proxy eingetragen werden muss und lokal auf dem Benutzer-PC ausge-	Sobald im Browser (sowohl Internet Explorer als auch Mozilla) ein externer Proxy-Server konfiguriert wird, ist bei aktiviertem Web-Proxy-Filter kein Internetzugriff mit dem Browser mehr möglich. Anders sieht die Sache aus, wenn anstelle eines externen Proxy-Servers ein lokaler Web-Proxy im Browser eingerichtet wird. Eine Verbindung ins Internet ist über diesen Proxy trotz aktiviertem Filter möglich. Verständlicherweise funktioniert auch der direkte Zugriff auf den Online-Web-Proxy	✓

[10] Free Proxy Public Servers List, siehe http://tools.rosinstrument.com/proxy/
[11] JAP Anonymity & Privacy, siehe http://anon.inf.tu-dresden.de/

Getestete Funktion	*Durchgeführte Tests*	*Ergebnisse / Erkenntnisse*
	führt wird ➢ Zugriffsversuche auf öffentlich frei zugänglichen Online-Web-Proxy[12] (keine Proxy-Einstellungen im Browser nötig)	im Internet ohne Probleme, da ja keine Proxy-Einstellungen direkt im Browser vorgenommen wurden.

Tabelle 7: ZyWALL 10W Content-Filtering – durchgeführte Tests und Ergebnisse

Im Bereich des URL-Filtering hat der Firewall-Administrator die Möglichkeit, die Zugriffsversuche für Angebote in den folgenden Kategorien aufzuzeichnen (zu loggen) und/oder zu blockieren:

Kategorie	*Erläuterungen*
Violence/Profanity	Umfasst gewalttätige Bilder und Texte gegen Menschen und Tiere
Gross Depictions	Umfasst vulgäre und unsittliche Bilder und Texte
Militant/Extremist	Umfasst ungesetzliche militante und/oder extremistische Bilder und Texte
Gambling/Questionable/Illegal	Umfasst Bilder und Texte mit dubiosem Charakter, welche unter Umständen illegal sind (inkl. Computer-Hacking und Software-Piraterie)
Partial Nudity	Umfasst Bilder, auf welchen die weibliche Brust und/oder das weibliche oder männliche Gesäss abgebildet sind
Full Nudity	Umfasst Bilder, auf welchen Genitalien abgebildet sind
Sexual Acts	Umfasst Texte und Bilder, welche sexuelle Handlungen beschreiben oder aufzeigen (inkl. Reklame für Telefonsex und Dating-Dienste und CD-ROMs und Videos mit entsprechendem Material)
Sex Education	Umfasst Texte und Bilder, welche den korrekten Gebrauch von Empfängnisverhütungsmitteln aufzeigen
Intolerance	Umfasst rassistische und anderweitig diskriminierende Texte und Bilder
Satanic/Cult	Umfasst Texte und Bilder, welche den Teufel anbeten oder irgend einen Kult propagieren
Alcohol/Tobacco	Umfasst Texte und Bilder, welche den Alkohol und den Tabak bewerben oder deren Konsum befürworten
Sports/Entertainment	Umfasst Texte und Bilder, welche mit der Freizeit und Sport und somit nichts mit dem Tagesgeschäft der Angestellten zu tun haben
Drug Culture	Umfasst Texte und Bilder, welche den illegalen Gebrauch von Drogen befürworten (ausgenommen der Drogen, die im medizinischen Umfeld Verwendung finden)

Tabelle 8: ZyWALL 10W – Filter-Kategorien für das URL-Filtering

[12] Guardster-Homepage, siehe http://www.guardster.com/

Damit das URL-Filtering aktiviert werden kann, muss sich der Firewall-Administrator zuerst bei ZyXEL registrieren lassen, danach kann eine so genannte Filterliste aus dem Internet heruntergeladen werden, welche die zu blockenden Angebote enthält. Dieser Dienst kann während eines halben Jahres kostenlos getestet bzw. verwendet werden (inkl. regelmässigen Filter-Listen-Updates), danach wird eine Gebühr fällig.

Beim Internet-Zugriff eines Benutzers wird bei aktiviertem URL-Filtering überprüft, ob sich das vom Benutzer angeforderte Web-Angebot in der Filterliste befindet. Wenn dies der Fall ist, erhält der Benutzer anstelle der Webseite einen Hinweis, welcher durch den Firewall-Administrator frei definiert werden kann. Wenn sich das angeforderte Angebot nicht in der Filterliste befindet, wird die Webseite ganz normal angezeigt.

Es lässt sich festlegen, wann (permanent oder nur zu bestimmten Tageszeiten) und für wen (einzelne IP-Adressenbereiche können von der Sperre ausgenommen werden) die entsprechenden Filter gelten sollen. Diese Einstellungen wirken sich jedoch immer sowohl auf das Content-Filtering (also das Blocken von Java-Applets, ActiveX-Controls usw.) als auch auf das URL-Filtering aus.

Das Handbuch zur Firewall lässt keine Rückschlüsse zu, welches Produkt für die Durchführung des URL-Filterings eingesetzt wird. Technische Untersuchungen im Rahmen dieser Diplomarbeit haben jedoch gezeigt, dass das Filtering der ZyWALL 10W auf dem Produkt „Cyber Patrol“[13] basiert. Diese technischen Untersuchungen haben aus Sicherheitsoptik darüber hinaus weitere interessante Erkenntnisse geliefert, welche im Anhang unter Kapitel 13.1.3 näher erläutert werden.

Um nun die Wirksamkeit der Filterfunktion zu testen, wurden diverse Tests durchgeführt, welche sich grundsätzlich auf alle Kategorien beziehen. Es wurde bewusst darauf verzichtet, jede Kategorie einzeln zu begutachten und zu bewerten. Die folgende Zusammenstellung gibt einen Überblick über die durchgeführten Versuche und den daraus resultierenden Ergebnissen:

Versuche / Aktivitäten	***Erkenntnisse / Ergebnisse***
➢ Alle URL-Filter-Kategorien aktivieren ➢ Im Internet gezielt Seiten aus den Bereichen „Erotik, Pornographie“ und „Computer-Hacking, Software-Piraterie“ unter der Eingabe des jeweiligen **DNS-Namens** ansurfen	Die Mehrheit der stichprobenweise ausgesuchten Web-Seiten im Erotikbereich werden zuverlässig geblockt. Es fällt hingegen auf, dass keine einzige angesurfte Website aus dem Bereich „Computer-Hacking, Software-Piraterie“ geblockt wird. Anscheinend wird durch den Filterhersteller dem Thema Erotik / Pornographie ein höherer Stellenwert zugemessen als dem Bereich Computer-Hacking / Software-Piraterie. ✓ ✘ Es gilt zu berücksichtigen, dass diese Erkenntnisse auf subjektiv vorgenommen Einzelstichproben und nicht auf einer repräsentativen umfangreichen Auswahl von Webseiten beruhen.
➢ Im Internet gezielt Seiten aus dem Bereich „Erotik, Pornographie“, welche im	Auch wenn Anstelle des DNS-Namens die IP-Adresse der Ziel-Webseiten verwendet wird, werden die angesurften Webseiten mit der gleichen ✓

[13] Cyber Patrol, siehe http://www.cyberpatrol.com

Versuche / Aktivitäten	***Erkenntnisse / Ergebnisse***	
ersten Versuch erfolgreich geblockt wurden, unter der Eingabe ihrer **IP-Adresse** ansurfen	Zuverlässigkeit geblockt wie beim ersten Versuch.	
➢ Im Internet gezielt Seiten aus dem Bereich „Erotik, Pornographie“, welche in den beiden ersten Versuchen erfolgreich geblockt wurden, unter der Eingabe ihrer **IP-Adresse als Dezimalzahl*** ansurfen	Auch wenn Anstelle des DNS-Namens oder der normalen IP-Adresse die IP-Adresse als Dezimalzahl verwendet wird, werden die angesurften Webseiten mit der gleichen Zuverlässigkeit geblockt wie bei den ersten beiden Versuchen.	✓
➢ Einrichten eines lokalen Web-Proxies[14], welcher im Browser als Proxy-Server eingetragen wird; im Internet gezielt Seiten aus dem Bereich „Erotik, Pornographie“, welche in den ersten drei Versuchen erfolgreich geblockt wurden, ganz normal über ihren DNS-Namen ansurfen	Sowohl unter der Verwendung eines lokalen Web-Proxies als auch über den getesteten Online-Web-Proxy „Guardster“ kann ohne Probleme auf alle Webseiten zugegriffen werden. Die Firewall „sieht“ nur die Verbindung (IP-Adresse) zu den Web-Proxy-Anbietern und hat keine Kenntnis von den letztlich angesurften Webseiten. Auf diese Weise kann sie den Zugriff auf die an und für sich nicht zugelassenen Webseiten auch nicht unterbinden.	
➢ Verbindung zu dem öffentlich frei zugänglichen Online-Web-Proxy „Guardster“[15] und zum „Web Page Backward Compatibility Viewer“[16] herstellen; über beide Dienste gezielt Seiten aus dem Bereich „Erotik, Pornographie“, welche in den ersten drei Versuchen erfolgreich geblockt wurden, ganz normal über ihren DNS-Namen ansurfen	Beim Zugriff auf nicht zugelassene Webseiten mittels dem „Web Page Backward Compatibility Viewer“ und dem „Google“-Übersetzungsdienst werden die Webseiten nicht geblockt; dem Benutzer werden jedoch nur die Textpassagen der nicht zugelassenen Webseiten, aber nicht die Bilder, angezeigt.	✓ ✘
➢ Webseiten aus dem Bereich „Erotik, Pornographie“, welche in den ersten drei Versuchen erfolgreich geblockt wurden, über die Suchmaschine „Google“[17] ausfindig machen und die-		

[14] JAP Anonymity & Privacy, siehe http://anon.inf.tu-dresden.de/
[15] Guardster-Homepage, siehe http://www.guardster.com/
[16] Web Page Backward Compatibility Viewer, siehe http://www.delorie.com/web/wpbcv.html
[17] Google-Suchmachine, siehe http://www.google.com

Versuche / Aktivitäten	*Erkenntnisse / Ergebnisse*
se mittels Übersetzungsdienst von „Google“ übersetzen lassen	

Tabelle 9: ZyWALL 10W URL-Filtering – durchgeführte Tests und Ergebnisse

* Dabei wird die normale IP-Adresse folgendermassen in eine Dezimalzahl umgewandelt:
Der Dezimalwert jedes Bytes der IP-Adresse 147.88.189.201 (hier als Beispiel die IP-Adresse der Internetseite der Hochschule für Wirtschaft in Luzern www.hsw.fhz.ch) wird in einen hexadezimalen Wert umgerechnet. Aus „147“ (Dezimal) wird somit „93“ (Hex), aus „88“ wird „58“, aus „189“ wird „BD“ und aus „201“ wird „C9“. Die einzelnen Hex-Werte werden nun aneinander gereiht, daraus entsteht „9358BDC9“. Dieser zusammengesetzte Hex-Wert wird danach in eine Dezimalzahl umgerechnet; daraus resultiert das Ergebnis „2472066505“. Die URL des Internetauftritts der Hochschule für Wirtschaft lautet in Dezimalzahlenform folglich „http://2472066505“. **Anmerkung:** Der Aufruf der Webseite in dieser Form kann mit allen Browsern, ausser mit dem Internet Explorer 6.0, erfolgreich durchgeführt werden. Der Internet Explorer 6.0 setzt die Dezimalzahl nicht in eine IP-Adresse um, sondern sucht mittels NetBIOS-Protokoll nach einem System mit dem Namen „2472066505“, welches natürlich nicht gefunden werden kann.

Da sich das Internetangebot laufend ändert und somit auch permanent neue Seiten im Internet zu finden sind, welche in eine der zu filternden Kategorien fallen, sollte die Filterliste regelmässig aktualisiert werden. Die Firewall bietet die Möglichkeit, die aktuelle Filterliste einmal wöchentlich zu einer frei definierbaren Zeit automatisch aus dem Internet herunterladen zu lassen. Ausserdem lässt sich die heruntergeladene Filter-Liste durch weitere Einträge manuell ergänzen. Diese Einträge erfolgen über die Firewall-Administrationsoberfläche. Eine direkte Bearbeitung der heruntergeladenen Filter-Liste ist nicht möglich. Die manuelle Ergänzung der Filter-Liste kann sehr zeitaufwendig sein, da, wie in Abbildung 2 ersichtlich, für einen effektiven Filter-Schutz neben dem Domänennamen der zu blockenden Internetseite auch ihre IP-Adresse sowohl in Normal- als auch Dezimalform eingetragen werden muss. Für einen umfassenden Zugriffsschutz sind somit pro Internetangebot drei manuelle Einträge nötig!

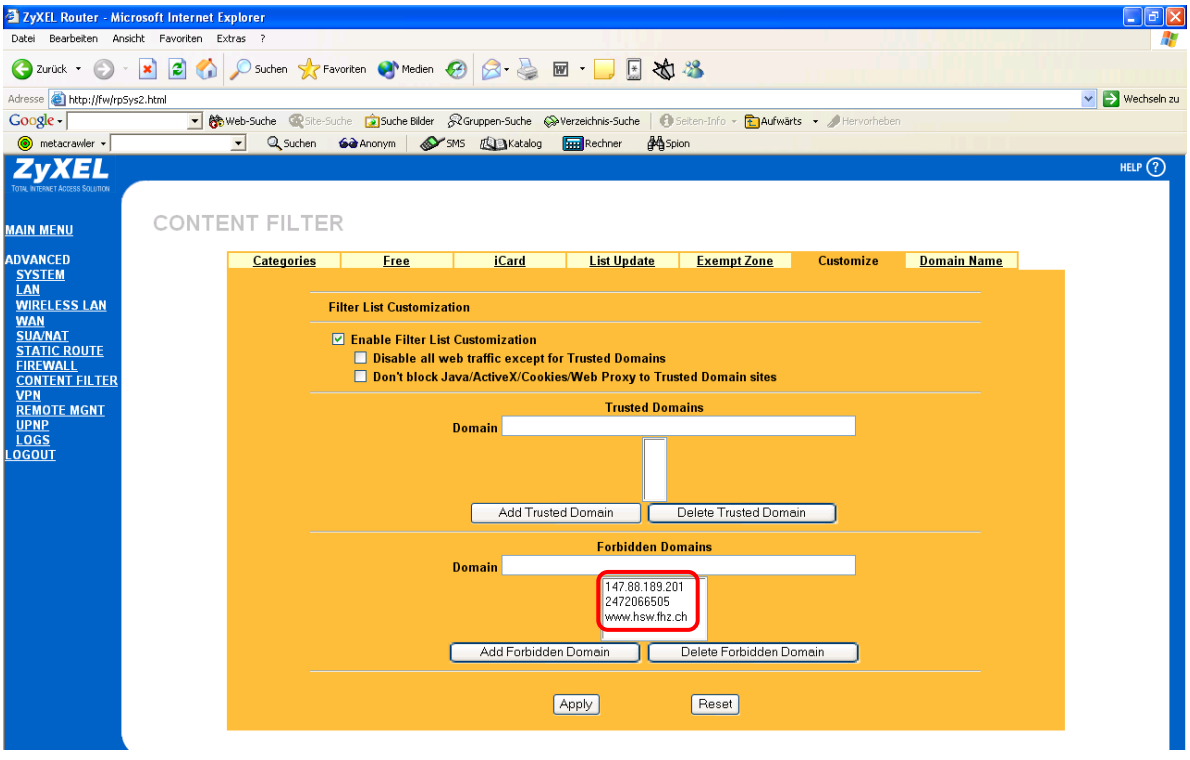


Abbildung 2: ZyWALL 10W URL-Filtering – manuelle Ergänzung der Filter-Liste

Zusätzlich besteht die Möglichkeit, vertrauenswürdige Domänen explizit zu definieren. Ein Zugriff auf diese Domänen ist danach, ungeachtet davon, ob sie in der URL-Filter-Liste stehen, uneingeschränkt möglich. Auf diese Weise lassen sich Java-Applets, ActiveX-Controls usw. (also die Elemente des Content-Filterings) für diese vertrauenswürdigen Domänen freischalten. Der gesamte erlaubte Internetzugriff kann jedoch auch auf die vertrauenswürdigen Domänen eingeschränkt werden, d.h. die Internet-Benutzer können dann nur noch auf diese Domänen zugreifen.

Als letzte Variante des Web-Seiten-Zugriffsschutzes kann der Firewall-Administrator definieren, welche Zeichenfolgen in der URL nicht vorkommen dürfen. So hat der Ausschluss der Zeichenfolge „hsw“ zur Folge, dass die Internetseite der Hochschule für Wirtschaft in Luzern über ihren Domänennamen „www.hsw.fhz.ch“ nicht mehr aufgerufen werden kann. Auch eine solche Sperre lässt sich natürlich problemlos umgehen, indem anstelle des Domänennamens direkt die IP-Adresse der Website eingegeben wird.

Fazit Content- und URL-Filtering

Die Möglichkeiten des Content- und URL-Filtering der Firewall hinterlassen einen zwiespältigen Eindruck. Das Cookie-Filtering als Bestandteil des Content-Filtering scheint nicht wie gewünscht wirksam zu sein. Das URL-Filtering steht und fällt mit dem Umfang, der Qualität und der Aktualität der Filter-Liste. Webseiten, welche nicht Gegenstand der Filter-Liste sind, können auch nicht gefiltert werden. Das trifft insbesondere auch für die öffentlichen Web-Proxy-Seiten zu. Diese stellen diesbezüglich ein besonders grosses Risiko dar, da bei einem erfolgreichen Zugriff auf einen solchen Anbieter der ganze Filter-Schutz umgangen werden kann und die Filter-Liste somit hinfällig wird. Die manuellen Erweiterungen im Bereich des URL-Filtering erscheinen nur bedingt praxistauglich, da der Zeitaufwand zur Erfassung und Pflege dieser Erweiterungen nicht unterschätzt werden darf und deren Wirksamkeit zum Teil mit trivialsten Mitteln untergraben werden kann.

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen 😐

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Die Firewall verfügt über Content-Filter für ActiveX-Controls, Java-Applets, Cookies und Web-Proxies
- Eine Vielzahl von URL-Filtering-Kategorien, welche einzeln aktiviert oder deaktiviert werden können, stehen zur Verfügung
- Die Einträge der URL-Filter-Liste können durch manuelle Einträge direkt auf der Firewall ergänzt werden
- Das URL-Filtering funktioniert bei den in der Filter-Liste vorhandenen Einträgen sowohl basierend auf dem DNS-Namen als auch basierend auf der IP-Adresse und der dezimalisierten IP-Adresse zuverlässig
- Einzelne Arbeitsstationen können vom Content- und URL-Filtering ausgenommen werden
- Auch wenn die Content- und URL-Filtering-Funktion

⊖

- Der Content-Filter für Cookies scheint ziemlich wirkungslos zu sein oder verhält sich auf jeden Fall nicht wie erwartet
- Die URL-Filter-Liste scheint nicht alle Filter-Kategorien gleich umfassend abzudecken; ein Schwergewicht besteht anscheinend auf dem Bereich „Erotik, Pornographie“
- Das Pflegen von manuellen URL-Filter-Einträgen ist sehr zeitaufwendig, da die Einträge für ein wirksames URL-Filtering immer in Form des DNS-Namens, der IP-Adresse und der dezimalisierten IP-Adresse eingegeben werden müssen
- Die Deaktivierung des Content- und URL-Filterings für eine Arbeitsstation wirkt sich immer sowohl für das Content- als auch das URL-Filtering aus. Eine unabhängige Aktivierung/Deaktivierung des Content- oder des URL-

⊕	⊖
nicht in allen Bereich zuverlässig und richtig funktioniert, vermag sie doch ihren Beitrag zu einer höherem Gesamtsicherheit zu leisten	Filterings ist nicht möglich ➢ In der URL-Filter-Liste sind anscheinend Online-Web-Proxy-Server bzw. -Dienste nicht vermerkt; deshalb können die URL-Filter umgangen werden ➢ Alle Content- und URL-Filter können mit einem lokalen Web-Proxy umgangen werden; der Einsatz eines lokalen Web-Proxies kann durch die Firewall nicht verhindert werden

5.3.2 „Intrusion Detection"-Funktionen, Anti-Spoofing

Mit der Funktion „Attack Alert" bietet die Firewall die Möglichkeit, allfällige DoS- (Denial of Service) und andere Attacken möglichst frühzeitig zu erkennen und zu loggen. Gemäss Firewall-Dokumentation[18] erkennt die Firewall folgende Attacken:

- DoS-Attacken
  - Ping of Death
  - Teardrop
  - SYN flooding
  - Land
  - Smurf
- IP Spoofing auf WAN-Interface
- Portscans
- ICMP-Attacken
- NetBIOS-Attacken

Je nach Konfiguration der Firewall registriert diese mit den Standard-Einstellungen jedoch bereits ganz normale Zugriffe aus dem internen Netzwerk auf das Internet als Attacke. Als Beispiel sei hier die vermeintliche „Ports Scan TCP"-Attacke erwähnt, welche die Firewall glaubt entdeckt zu haben (siehe Abbildung 3). Wie in der Abbildung zu sehen ist, erfolgt der Zugriff aus dem internen Netzwerk mit der privaten IP-Adresse 192.168.27.11 auf die öffentliche IP-Adresse 195.65.57.119 (Web-Shop mit SSL-Verschlüsselung). Diese vermeintlichen Attacken werden durch die Firewall jedoch nur registriert, wenn sie sich hinter einem ADSL-Router befindet, welcher selber auch ein Routing durchführt. Sobald auf dem ADSL-Router der Bridging-Modus konfiguriert wird (ein Routing wird nun nur noch auf der Firewall durchgeführt), meldet die Firewall keine „falschen" Attacken mehr (bezüglich Routing- und Bridging-Modus des ADSL-Routers siehe die Ausführungen unter 5.3.7).

[18] vgl. ZyWALL 10/10W/50/100 User's Guide, Dez. 2002

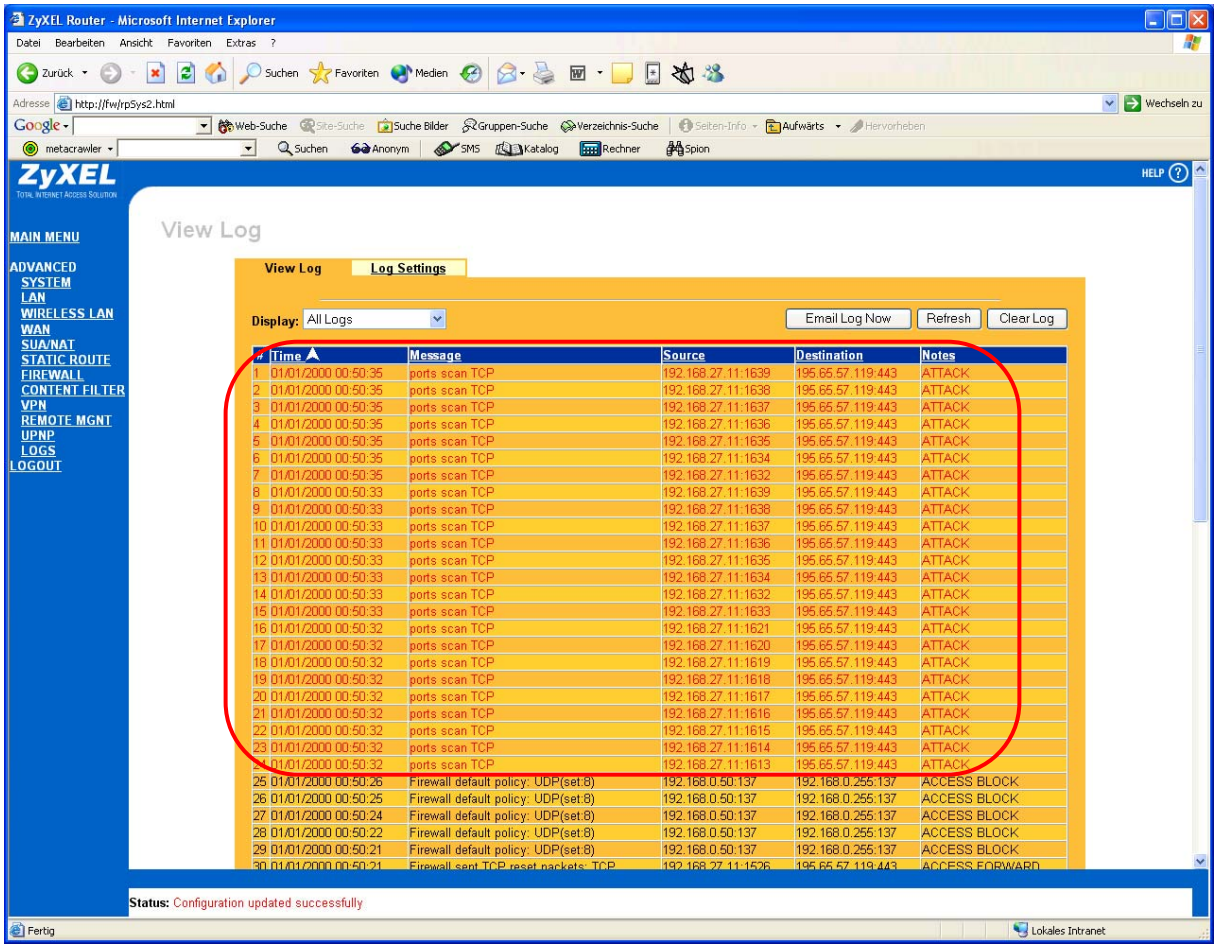


Abbildung 3: ZyWALL 10W – Durch die Firewall gemeldete vermeintliche Attacken beim Zugriff auf das Internet

Eine andere Möglichkeit, Fehlalarme bezüglich vermeintlicher Attacken zu verhindern, besteht darin, einen Schwellenwert in der Attacken-Konfiguration der Firewall zu ändern. Der Eintrag „TCP Maximum Incomplete“ weist standardmässig einen Schwellenwert von „10“ auf (siehe Abbildung 4). Dieser Wert bedeutet, dass maximal 10 halb-offene Sessions mit der gleichen Ziel-IP-Adresse bestehen dürfen. Als halb-offene Sessions gelten Sessions, bei welchen das „TCP-3-way-handshake“ (syn, syn/ack, ack) noch nicht vollständig durchgeführt wurde. Falls mehr als 10 halb-offene Sessions mit der gleichen Ziel-IP-Adresse bestehen, interpretiert das die Firewall als „Portscan“-Attacken gegen das Ziel-System. Eine Erhöhung dieses Schwellenwerts von „10“ auf „30“ reichte für den oben erwähnten Web-Shop (IP-Adresse 195.65.57.119) bereits aus, um falsche Attacken-Meldungen zu verhindern.

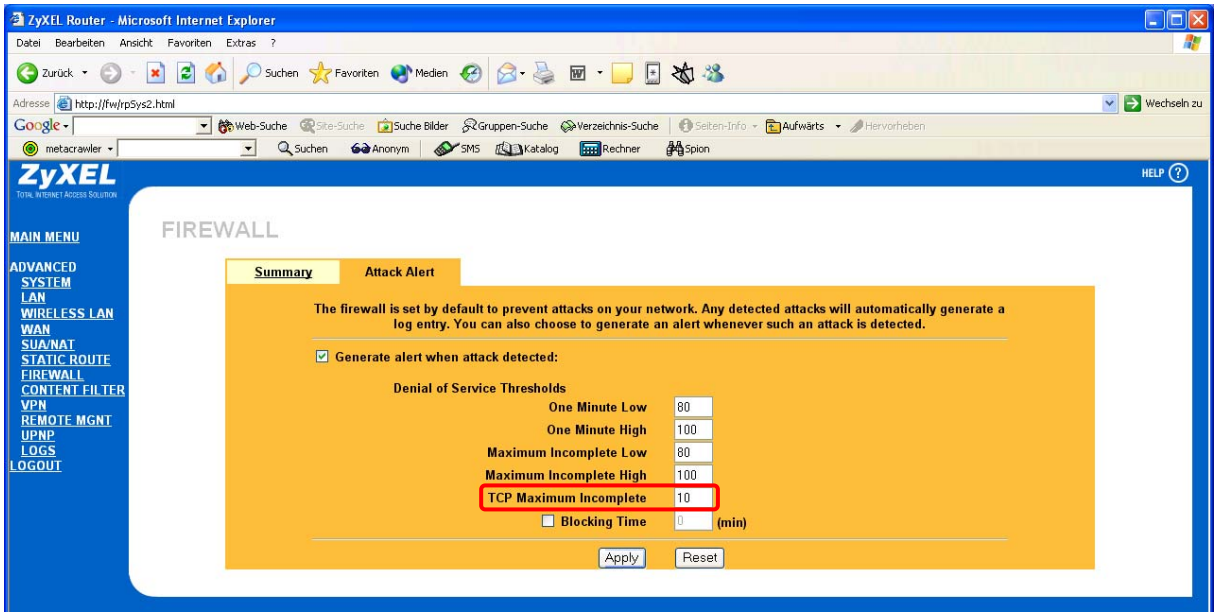


Abbildung 4: ZyWALL 10W – Konfiguration der Attacken-Schwellenwerte

Nun stellt sich natürlich die Frage, inwiefern die Veränderung des Schwellwerts zur Vermeidung von Fehlalarmen bei Zugriffen aus dem internen Netzwerk auf das Internet die Wirksamkeit der „Intrusion Detection"-Funktion bezüglich Erkennung von effektiven Attacken, welche vom externen Netzwerk her erfolgen und das interne Netzwerk zum Ziel haben, beeinflusst. Einige Versuche mit gezielten Portscans[19] haben folgendes Ergebnis geliefert:

Art des Portscans	***Quell-System***	***Ziel-System***	***TCP Maximum Incomplete***	***Resultate / Bemerkungen***
Portscan „Connect" *	192.168.0.50 (äusseres Netz)	192.168.27.11 (inneres Netz, NAT auf Firewall)	1 – 4	Die Firewall erkennt bei einem tiefen Schwellenwert des „TCP Maximum Incomplete"-Parameters eine „TCP-Portscan"-Attacke, weil die beim durchgeführten Portscan parallel vorhandenen halb-offenen Sessions den Schwellenwert überschreiten. ✓
Portscan „Connect" *	192.168.0.50 (äusseres Netz)	192.168.27.11 (inneres Netz, NAT auf Firewall)	> 4	Bereits ab einem (nach wie vor tiefen) Schwellenwert von 5 des „TCP Maximum Incomplete"-Parameters vermag die Firewall die Portscan-Attacke nicht mehr zu erkennen. ✗
Portscan „SYN Stealth" *	192.168.0.50 (äusseres Netz)	192.168.27.11 (inneres Netz, NAT auf Firewall)	< 26	Bei einem „SYN Stealth"-Portscan erkennt die Firewall in jedem Fall eine Attacke, da kein kompletter „TCP-3-way-handshake" durchgeführt wird. Bei einem Schwellenwert < 26 des „TCP Maximum Incomplete"-Parameters meldet die Firewall eine „TCP-Portscan"-Attacke ✓
Portscan „SYN Stealth" *	192.168.0.50 (äusseres Netz)	192.168.27.11 (inneres Netz, NAT auf Firewall)	> 25	Bei einem „SYN Stealth"-Portscan und einem „TCP Maximum Incomplete"-Schwellenwert > 25 meldet die Firewall hingegen eine „SYN-Flood-TCP"-Attacke. ✓

[19] Die Portscans wurden mit dem Programm „nmap" durchgeführt (www.insecure.org)

Art des Portscans	***Quell-System***	***Ziel-System***	***TCP Maximum Incomplete***	***Resultate / Bemerkungen***
Portscan „connect“ *	192.168.0.50 (äusseres Netz)	192.168.0.20 (External Interface Firewall)	1 – 250 (max. Wert)	Den Portscan direkt auf das äussere Interface der Firewall meldet die Firewall in der Log-Datei als „Access block“, jedoch nicht als Attacke. ✘
Portscan „SYN Stealth“ *	192.168.0.50 (äusseres Netz)	192.168.0.20 (External Interface Firewall)	1 – 250 (max. Wert)	Den Portscan direkt auf das äussere Interface der Firewall meldet die Firewall in der Log-Datei als „Access block“, jedoch nicht als Attacke. ✘

Tabelle 10: ZyWALL 10W "Intrusion Detection" – Resultate diverser Portscans auf die Firewall

* Ergänzende Erläuterungen zur Tabelle

- Bei einem „Connect“-Portscan wird ein kompletter „TCP-3-way-handshake“ (syn, syn/ack, ack) durchgeführt.
- Bei einem „SYN Stealth“-Portscan wird kein kompletter „TCP-3-way-handshake“ durchgeführt. Die Verbindung wird vor dem Abschluss des kompletten „TCP-3-way-handshake“ abgebrochen.

Es fällt auf, dass einerseits die Höhe des Schwellenwertes des „TCP Maximum Incomplete“-Parameters und andererseits die Art des durchgeführten Portscans einen grossen Einfluss darauf haben, ob die Firewall den Portscan als Attacke taxiert oder nicht. Ein Portscan, welcher ein komplettes „TCP-3-way-handshake“ durchführt, wird von der Firewall grundsätzlich nicht als solcher wahrgenommen.

Aufgrund der durchgeführten Tests und der daraus resultierenden Ergebnisse darf die Zuverlässigkeit der integrierten „Intrusion Detection“-Funktion angezweifelt werden.

Wenigstens wurden die Versuche betreffend IP-Spoofing auf dem externen Interface (Verwendung der internen IP-Adresse 192.168.27.80 auf dem externen Firewall-Interface mit der IP-Adresse 192.168.0.20) korrekt von der Firewall erkannt:

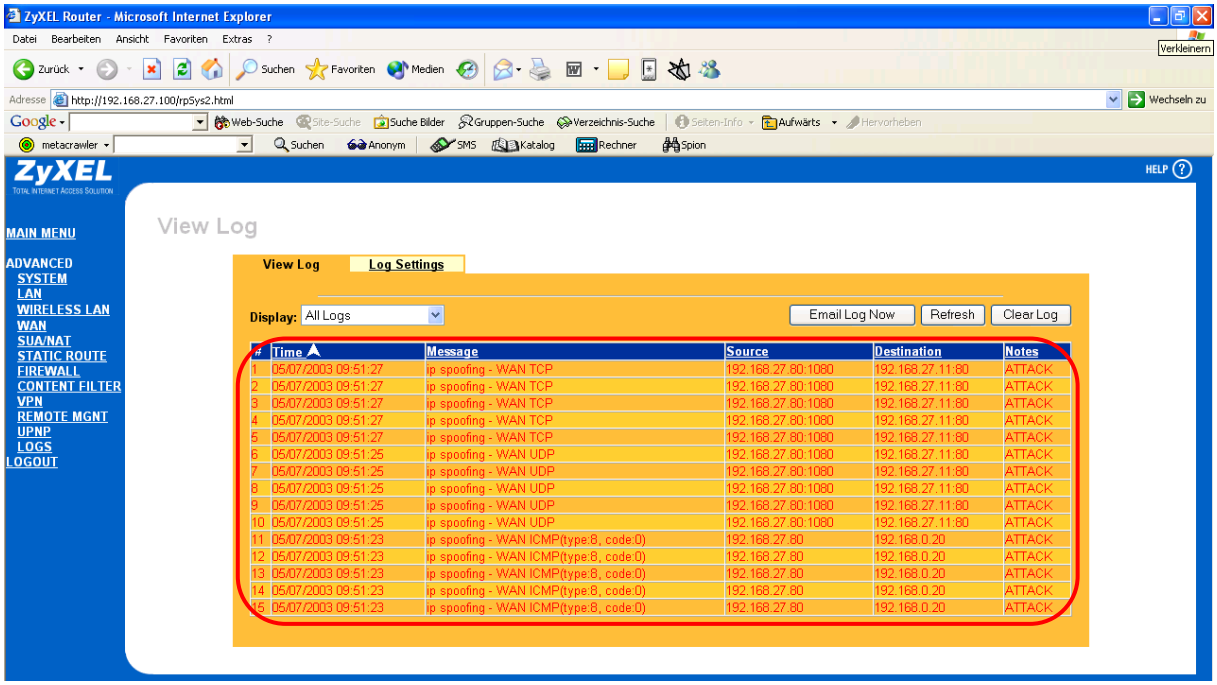

ZyXEL Router - Microsoft Internet Explorer
ZyXEL
HELP
MAIN MENU
ADVANCED
SYSTEM
LAN
WIRELESS LAN
WAN
SUA/NAT
STATIC ROUTE
FIREWALL
CONTENT FILTER
VPN
REMOTE MGNT
UPNP
LOGS
LOGOUT
View Log
View Log
Log Settings
Display: All Logs
Email Log Now
Refresh
Clear Log
Time Message Source Destination Notes
1 05/07/2003 09:51:27 ip spoofing - WAN TCP 192.168.27.80:1080 192.168.27.11:80 ATTACK
2 05/07/2003 09:51:27 ip spoofing - WAN TCP 192.168.27.80:1080 192.168.27.11:80 ATTACK
3 05/07/2003 09:51:27 ip spoofing - WAN TCP 192.168.27.80:1080 192.168.27.11:80 ATTACK
4 05/07/2003 09:51:27 ip spoofing - WAN TCP 192.168.27.80:1080 192.168.27.11:80 ATTACK
5 05/07/2003 09:51:27 ip spoofing - WAN TCP 192.168.27.80:1080 192.168.27.11:80 ATTACK
6 05/07/2003 09:51:25 ip spoofing - WAN UDP 192.168.27.80:1080 192.168.27.11:80 ATTACK
7 05/07/2003 09:51:25 ip spoofing - WAN UDP 192.168.27.80:1080 192.168.27.11:80 ATTACK
8 05/07/2003 09:51:25 ip spoofing - WAN UDP 192.168.27.80:1080 192.168.27.11:80 ATTACK
9 05/07/2003 09:51:25 ip spoofing - WAN UDP 192.168.27.80:1080 192.168.27.11:80 ATTACK
10 05/07/2003 09:51:25 ip spoofing - WAN UDP 192.168.27.80:1080 192.168.27.11:80 ATTACK
11 05/07/2003 09:51:23 ip spoofing - WAN ICMP(type:8, code:0) 192.168.27.80 192.168.0.20 ATTACK
12 05/07/2003 09:51:23 ip spoofing - WAN ICMP(type:8, code:0) 192.168.27.80 192.168.0.20 ATTACK
13 05/07/2003 09:51:23 ip spoofing - WAN ICMP(type:8, code:0) 192.168.27.80 192.168.0.20 ATTACK
14 05/07/2003 09:51:23 ip spoofing - WAN ICMP(type:8, code:0) 192.168.27.80 192.168.0.20 ATTACK
15 05/07/2003 09:51:23 ip spoofing - WAN ICMP(type:8, code:0) 192.168.27.80 192.168.0.20 ATTACK

Abbildung 5: ZyWALL 10W – Erkennung von IP-Spoofing-Angriffen

Demgegenüber wird ein IP-Spoofing auf dem internen Interface (Verwendung der externen IP-Adresse 192.168.0.60 auf dem internen Firewall-Interface mit der IP-Adresse 192.168.27.100) durch die Firewall nicht festgestellt.

Fazit „Intrusion Detection"-Funktion, Anti-Spoofing

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs

- Die Firewall versucht, allfällige DoS- oder andere Attacken möglichst frühzeitig zu erkennen
- IP-Spoofing wird auf dem externen Interface der Firewall erkannt
- Auch wenn die „Intrusion Detection"-Funktion nicht immer zuverlässig ist, vermag sie doch ihren Beitrag zu einer höheren Gesamtsicherheit zu leisten

- Die Firewall liefert einige „False Positives" (z.B. Meldung eines Portscans bei ganz normalen Internet-Zugriffen)
- Die Firewall liefert einige „False Negatives" (z.B. wird ein „Connect"-Portscan meistens nicht als solcher erkannt)
- Portscans direkt auf die Firewall werden nicht als solche erkannt
- IP-Spoofing auf dem internen Interface der Firewall wird nicht erkannt

5.3.3 Logging-Möglichkeiten und Alarmierung

Die Log-Einträge werden in verschiedene Kategorien unterteilt. Die Kategorien bilden gleichzeitig auch die Filter, nach welchen die Log-Einträge am Bildschirm ausgegeben werden können. Natürlich ist es auch möglich, sich das gesamte Log ungefiltert anzeigen zu lassen. Nachfolgende Tabelle gibt einen Überblick über die vorhandenen Kategorien und ob bei einem neuen Log-Eintrag in eine der Kategorien ein unmittelbarer Alarm an eine E-Mail-Adresse ausgelöst werden kann oder nicht:

Bezeichnung des Logs	***Erläuterungen zum Inhalt***	***Unmittelbare Alarmierung möglich***
System Maintenance	Hinweise zum Zeitabgleich, zum DHCP-Server und zu Firewall-Administrator-Logins (via Konsole, Telnet, FTP, WWW).	nein
System Errors	Fehlermeldungen, falls versucht wird die maximale Anzahl der erlaubten NAT-Session-Tabelleneinträge zu überschreiten.	ja
Access Control	Einträge zu Paketen, welche aufgrund der Firewall-Regeln aufgezeichnet wurden.	ja
UPnP	Hinweise, falls UPnP (Universal Plug and Play) durch die Firewall erlaubt ist.	nein
Forward Web Sites	Einträge der Webseiten, auf welche die Benutzer erfolgreich zugreifen konnten.	nein

Bezeichnung des Logs	***Erläuterungen zum Inhalt***	***Unmittelbare Alarmierung möglich***
Blocked Web Sites	Einträge der Seiten, welche aufgrund des URL-Filtering geblockt wurden.	ja
Blocked Java etc.	Einträge der Seiten, welche aufgrund des Content-Filtering geblockt wurden.	ja
Attacks	Einträge von festgestellten Attacken der „Intrusion Detection"-Funktion (siehe dazu auch Kapitel 5.3.2).	ja
IPSec	Fehler und Hinweise in Zusammenhang mit dem Einsatz von VPN (Initialisierung der VPN-Session, Probleme im Bereich der Security Association usw.).	ja
IKE	Fehler und Hinweise in Zusammenhang mit dem Internet Key Exchange (IKE) beim Einsatz von VPN.	ja

Tabelle 11: ZyWALL 10W – Logging-Kategorien

Jede Kategorie kann für das Logging und, dort wo vorhanden, auch für die Alarmierung einzeln aktiviert oder deaktiviert werden. Der Informationsgehalt der einzelnen Log-Einträge (Datum, Uhrzeit, kurze Meldung, Quell-Adresse und Quell-Port, Ziel-Adresse und Ziel-Port, kurze Notiz) entspricht den minimalen Anforderungen. Die Log-Datei auf der Firewall umfasst über alle Kategorien hinweg maximal 128 Einträge. Mit dem 129. Eintrag wird automatisch der älteste Log-Datei-Eintrag überschrieben. Je nachdem, was alles geloggt wird, ist die Datei innerhalb kürzester Zeit voll. Zum Glück besteht die Möglichkeit, die Log-Einträge, sobald die Log-Datei voll ist oder in einem anderen zu definierenden Intervall, automatisch an eine E-Mail-Adresse zu versenden oder noch besser direkt an einen Syslog-Server weiterzuleiten.

Fazit Logging-Möglichkeiten und Alarmierung

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen 😐

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Verschiedene Log-Kategorien stehen zur Verfügung, welche einzeln aktiviert oder deaktiviert werden können
- Log-Einträge können nach verschiedenen Kategorien gefiltert werden
- Unmittelbare Alarmierung einzelner Ereignisse möglich
- Die Log-Einträge können automatisiert an eine E-Mail-Adresse und/oder einen Syslog-Server gesendet werden

⊖

- In den Log-Einträgen kann nicht gesucht werden (nur über die normale Suchfunktion des Internet-Browsers)
- Die Log-Datei nimmt maximal 128 Einträge auf, danach wird der älteste Einträg durch den neusten überschrieben

5.3.4 Network Address Translation (NAT)

Die ZyXEL ZyWALL 10W bietet sehr viele NAT-Konfigurationsmöglichkeiten. Grundsätzlich wird sowohl dynamisches als auch statisches NAT unterstützt, wobei einige Varianten zur Auswahl stehen. Folgende Tabelle gibt einen Überblick über die NAT-Konfigurationsmöglichkeiten:

NAT-Bezeichnung ZyXEL	Typ	Interne IP-Adresse(n)	Externe IP-Adresse(n)
One to One	statisch	192.168.1.10	80.254.159.30
Many to One	dynamisch	192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 […]	80.254.159.30
Many to Many Overload	Kombination zwischen statisch & dynamisch	192.168.1.10 192.168.1.11 192.168.1.12	80.254.159.30 80.254.159.31 80.254.159.32
Many One to One	statisch	192.168.1.10 192.168.1.11 192.168.1.12	80.254.159.30 80.254.159.31 80.254.159.32
Server	statisch	192.168.1.10 (Port 80) 192.168.1.20 (Port 25)	80.254.159.30 (Port 80) 80.254.159.30 (Port 25)

Tabelle 12: ZyWALL 10W – NAT-Konfigurationsmöglichkeiten

Vor allem die NAT-Variante „Server“ erscheint interessant, da auf diese Weise einer öffentlichen IP-Adresse je nach Dienst (Port) ein unterschiedliches internes Zielsystem (mit privater IP-Adresse) zugeordnet werden kann. Auf diese Weise ist es auch Benutzern, welche lediglich über eine öffentliche IP-Adresse verfügen (z.B. ADSL-Benutzer mit dynamischer öffentlicher IP-Adresse, welche diese vom ISP erhalten), möglich, Server-Dienste auf verschiedenen Systemen im Internet anzubieten. Es gilt jedoch zu berücksichtigen, dass sich dabei die Server-Systeme im gleichen Netzwerk wie die anderen Systeme befinden. Eine solche Konstellation ist aus Sicherheitsoptik allerdings nicht zu empfehlen.

<u>Fazit NAT</u>

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs –

⊕

- Die Firewall unterstützt sehr viele NAT-Konfigurationsmöglichkeiten bzw. -Varianten

⊖

- Allfällig angebotene Server-Dienste im internen Netzwerk stellen ein gewisses Risiko dar

- Durch NAT sind die internen Systeme aus dem Internet nicht direkt ersichtlich

5.3.5 DHCP-Server

Der DHCP-Server lässt sich aktivieren und deaktivieren. Folgende Einstellungen sind möglich:

- Startadresse des Bereichs der zu vergebenden IP-Adressen
- Grösse des Bereichs der zu vergebenden IP-Adressen
- IP-Adressen des ersten und des zweiten DNS-Servers

Die IP-Adresse des internen Interface der Firewall wird dem DHCP-Client als „Default-Gateway“ mitgeteilt.

Ausserdem können für einzelne Clients auch statische IP-Adressen vergeben werden (so genanntes statisches DHCP). Dabei erfolgt die Zuteilung der immer gleichen IP-Adresse aufgrund der Hardwareadresse (MAC-Adresse) der Netzwerkkarte des Clients.

Fazit DHCP-Server

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen	☺
Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs	-

- Alle wesentlichen DHCP-Einstellungen können vorgenommen werden
- Es wird sowohl dynamisches als auch statisches DHCP unterstützt

5.3.6 Zeitserver-Dienst

Die ZyWALL 10W kann ihre Systemzeit von einem Zeitserver beziehen. Dabei stehen verschiedene Protokolle (Daytime, Time, NTP) zur Verfügung. Der DNS-Name oder die IP-Adresse des Zeitservers lässt sich beliebig wählen. Somit besteht die Möglichkeit, die Zeit von einem Zeitserver im eigenen Netzwerk oder von einem Zeitserver aus dem Internet zu beziehen. Die Einstellung der eigenen Zeitzone und die Definition zum automatischen Umstellen der Systemzeit beim Wechsel von Sommer- auf Winterzeit und umgekehrt sind ebenfalls möglich, wobei die Flexibilität bei letztgenannter Option zu wünschen übrig lässt. Es besteht nur die Möglichkeit zu definieren, in an welchem Tag der entsprechenden Monate die Zeit umgestellt werden soll. Da sich die Tage, an welchen von Sommer- auf Winterzeit und von Winter- auf Sommerzeit umgestellt wird, jedoch von Jahr zu Jahr ändern, haben die entsprechenden Einstellungen nur gerade für ein Jahr Gültigkeit. Falls die Steuerung betreffend Sommer-/Winterzeit-Umschaltung nicht direkt durch den Zeitserver sondern durch die Firewall selber vorgenommen wird, ist eine jährliche Anpassung der Einstellungen auf der

Firewall nötig. Die Firewall aktualisiert ihre Zeit beim Einschalten des Geräts oder im 24-Stunden-Intervall.

Fazit Zeitserver

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Firewall kann Systemzeit sowohl von Zeitservern aus dem Internet als auch von Zeitservern aus dem internen Netzwerk beziehen
- Firewall und die wesentlichen internen Serversysteme erhalten alle ihre Systemzeit von einem zentralisierten Zeitserver, was die Nachvollziehbarkeit bei Zwischenfällen erhöht (erhöhte Sicherheit)

⊖

- Die Einstellungsmöglichkeiten bezüglich Wechsel der Uhrzeit von Sommer- auf Winterzeit und umgekehrt sind zu wenig flexibel

5.3.7 Dynamisches DNS

Die Firewall unterstützt den dynamischen DNS-Anbieter „dyndns.org“. Ein anderer Anbieter kann nicht ausgewählt werden. Nach Aktivierung dieses Dienstes in der Firewall und nach entsprechender Registration bei „dyndns.org“ funktioniert der automatische Update-Vorgang grundsätzlich problemlos. Voraussetzung ist jedoch, dass dem externen Interface der Firewall die dynamische öffentliche IP-Adresse des ISPs zugeordnet wurde (siehe Abbildung 6). Diese Voraussetzung erweist sich je nach Infrastruktur jedoch als „Konfigurations-Knacknuss“.

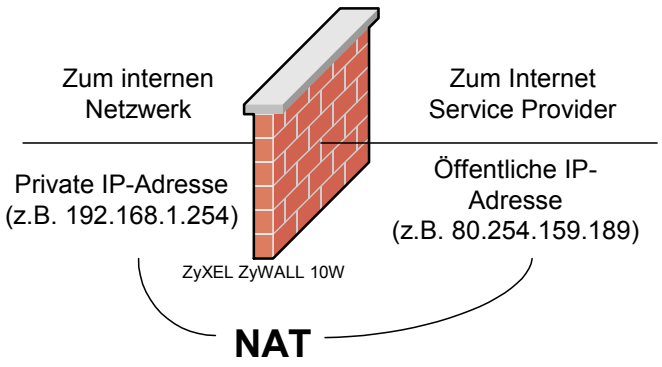


Abbildung 6: ZyWALL 10W mit öffentlicher WAN-IP-Adresse für dynamisches DNS

In den KMUs wird eine solche Firewall oft hinter einem ADSL-Router betrieben. Häufig wird dem externen Interface des ADSL-Routers die dynamische öffentliche IP-Adresse des ISPs zugewiesen. Das interne Interface des ADSL-Routers besitzt eine private IP-Adresse. Der ADSL-Router übersetzt dabei die internen privaten IP-Adressen mittels NAT in die externe öffentliche IP-Adresse. Die Firewall hinter dem ADSL-Router ist bezüglich IP-Adressen grundsätzlich ähnlich konfiguriert wie der Router, d.h. das externe Interface der Firewall besitzt eine private IP-Adresse aus dem gleichen Teilnetz, in dem sich auch die IP-Adresse des internen Interface des ADSL-Routers befindet und das interne Interface der Firewall verfügt

über eine private IP-Adresse aus dem Adressbereich des internen Netzwerks der Unternehmung. Falls auf der Firewall selber auch NAT konfiguriert ist (siehe Abbildung 7), übersetzt die Firewall analog zum ADSL-Router die IP-Adressen aus dem internen Netzwerk der Unternehmung. Andernfalls, wenn auf der Firewall kein NAT konfiguriert ist, werden die IP-Adressen aus dem internen Netzwerk einfach ganz normal durch die Firewall geroutet und die Übersetzung dieser erfolgt dann einzig und alleine auf dem ADSL-Router. So oder so, auf diese Weise verfügt das externe Interface der Firewall nicht, wie für den automatischen Update des dynamischen DNS-Dienstes erforderlich, über die dynamische öffentliche IP-Adresse des ISPs. Das Update muss deshalb jeweils manuell erfolgen.

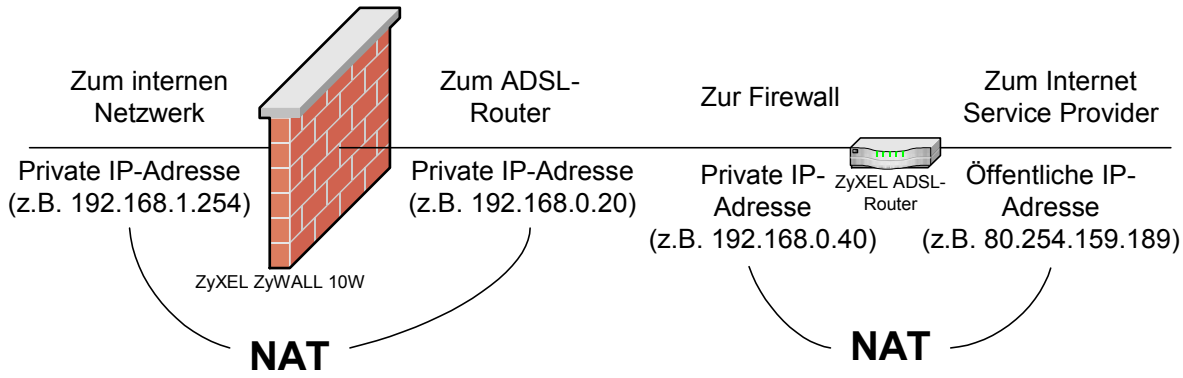


Abbildung 7: ZyWALL 10W mit privater WAN-IP-Adresse (dynamisches DNS nur eingeschränkt möglich)

Um dieses Problem zu lösen, ist der ADSL-Router in den so genannten Bridging-Modus zu setzen[20], damit der Router selber kein Routing mehr durchführt. Im Bridging-Modus wird die dynamische öffentliche IP-Adresse des ISPs automatisch vom ADSL-Router an das externe Interface der Firewall weitergereicht. Der Router fungiert so gesehen nicht mehr als ADSL-Router sondern „nur" noch als ADSL-Modem. Ausserdem wird die „Network Address Translation" (NAT) nur noch einmal, nämlich auf der Firewall, durchgeführt. Mit dieser Konfiguration funktioniert das automatische Update des „dyndns.org"-Dienstes nun problemlos.

<u>Fazit dynamisches DNS</u>

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☹

⊕

- Obschon die öffentliche IP-Adresse von Zeit zu Zeit ändert, können Server-Dienste unter dem immer gleichen DNS-Namen angesprochen werden
- Firewall kann den Update der jeweils aktuellen öffentlichen IP-Adresse beim dynamischen DNS-Anbieter bei richtiger Konfiguration automatisch durchführen

⊖

- Die mittels dynamischem DNS angebotenen Server-Dienste befinden sich auf Systemen (Servern) im internen Netzwerk, da die Firewall über keinen DMZ-Port verfügt. Dies stellt ein Sicherheitsrisiko für die übrigen internen Systeme dar

[20] Nähere Erläuterungen zur entsprechenden Konfiguration am Beispiel eines ZyXEL Prestige 642R ADSL-Routers sind im Anhang unter Kapitel 13.2.1 zu finden

5.3.8 Wireless-LAN (WLAN)

Die ZyWALL 10W wird standardmässig mit einer Wireless-LAN-Option ausgeliefert. Das bedeutet, dass die Firewall über einen PCMCIA-Steckplatz verfügt, in welchen eine Wireless-LAN-Netzwerkkarte nach dem IEEE 802.11b Standard eingesetzt werden kann. Gemäss Handbuch zur Firewall kann dabei eine ZyXEL-eigene WLAN-Karte oder aber irgendeine 802.11b-kompatible WLAN-Karte verwendet werden. Versuche haben jedoch gezeigt, dass keine der drei ausprobierten WLAN-Karten von Drittherstellern (Cisco Aironet 340, Siemens I-Gate 11M und Compaq WL110) von der Firewall erkannt wurde. Die Wireless-LAN-Option liess sich erst beim Einführen einer ZyXEL ZyAIR B-100 Wireless-LAN-Karte erfolgreich aktivieren.

Die Wireless-LAN-Einstellungen, die auf der Firewall vorgenommen werden können, entsprechen mehrheitlich den Optionen, welche heutzutage alle guten Wireless-LAN-Accesspoints bieten. Dazu gehören unter anderem:

- Freie Wahl der ESSID (Extended Service Set Identification ⇨ entspricht in etwa dem Netzwerknamen des WLANs)
- Möglichkeit, die ESSID zu verstecken, damit diese von einem potentiellen Angreifer nicht ohne weiteres erkannt werden kann (Unterdrückung der ESSID in den ausgehenden so genannten Beacon-Frames)
- Wahl des Kanals (es stehen 13 Kanäle zur Verfügung)
- WEP-Verschlüsselung (Wired Equivalent Privacy) mit 64-Bit oder 128-Bit Schlüssel. Bis zu 4 Schlüssel können definiert werden.
- MAC-Filter: Wireless-LAN-Karten, deren Netzwerkkarten-Hardwareadressen (MAC-Adressen) erfasst wurden, können entweder mit der Firewall kommunizieren (Allow Association) oder haben die Erlaubnis nicht, mit der Firewall zu kommunizieren (Deny Association)
- Netzwerk-Authentisierung: Der Wireless-Benutzer muss sich vor einem Zugriff auf das LAN authentisieren (nach dem IEEE 802.1x Standard). Dabei kommen das Protokoll EAP (Extensible Authentication Protocol) und als Option ein RADIUS-Server (Remote Authentication Dial-In User Service) zum Einsatz. Auf dem RADIUS-Server sind alle Wireless-Benutzer zentral erfasst. Bevor ein Zugriff auf das LAN erfolgt, muss sich ein Wireless-Benutzer mit seinem Benutzernamen und Passwort erfolgreich am RADIUS-Server anmelden. Die Firewall nimmt dabei die Funktion des RADIUS-Clients war. Für den Fall, dass kein RADIUS-Server zur Verfügung steht, können bis zu 32 Benutzer in einer lokalen Benutzerdatenbank direkt auf der Firewall verwaltet werden.

Dem Autor gelang es jedoch nicht, die letztgenannte Funktion erfolgreich in Betrieb zu nehmen. Alle durchgeführten Konfigurationsversuche, die Authentisierung mittels EAP direkt an der Firewall (ohne RADIUS-Server) vorzunehmen, schlugen fehl. Das Benutzerhandbuch[21] zur Firewall bietet diesbezüglich kaum Hilfe und zeigt nicht auf, wie der Authentisierungsprozess mittels EAP effektiv durchgeführt werden kann. Es wird lediglich erwähnt, dass der IEEE 802.1x Standard durch Windows XP und einige Netzwerk-Geräte unterstützt werde. Recherchen im Internet haben ergeben, dass Microsoft für das Windows 2000 Betriebsystem einen 802.1x-Patch anbietet, welcher es ermöglichen sollte, Authentisierungen basierend auf dem EAP-Protokoll vorzunehmen. Nach dem Herunterladen und der Installation dieses Patchs erschien beim Anmeldeversuch mittels EAP am Firewall-Accesspoint zwar ein Anmeldefenster, in welchem der Benutzername und das Passwort eingegeben werden konnten, der Authentisierungsvorgang wurde jedoch mit einer Fehlermeldung quittiert. Auch die

[21] vgl. ZyWALL 10/10W/50/100 User's Guide, Dez. 2002

Installation eines 802.1x-Clients eines Drittherstellers unter Windows 2000 (Odyssey Client[22]) brachte leider keinen Erfolg.

In einem solchen Fall muss auf die benutzerspezifische Authentisierung verzichtet werden und die Sicherheitseigenschaften des WLAN-Accesspoints in der Firewall werden auf die klassischen Massnahmen wie MAC-Adressfilter und WEP-Verschlüsselung reduziert. Dabei stellt sich jedoch die Frage, ob diese Schutzmassnahmen den grundsätzlichen Sicherheitsanforderungen genügen können. Bei aktiviertem DHCP-Server auf der Firewall (dabei handelt es sich um den gleichen DHCP-Server, welcher allenfalls auch den übrigen fix verkabelten internen Systemen IP-Adressen zuteilt) erhält ein WLAN-Benutzer, welcher über eine WLAN-Karte mit der korrekten MAC-Adresse und den WEP-Schlüssel verfügt, automatisch eine interne IP-Adresse zugeteilt; der WLAN-Benutzer befindet sich somit direkt im internen Netzwerk und hat dadurch von der Firewall unbehelligt Zugriff auf die anderen internen Systeme. In Anbetracht dessen, dass sich die MAC-Adresse problemlos fälschen lässt und auch der WEP-Schlüssel erfolgreich geknackt werden kann, scheint der Einsatz eines WLAN-Accesspoints direkt auf der Firewall je nachdem doch als ein eher riskantes Unterfangen.

Untenstehende Abbildung[23] zeigt die verschiednen Wireless-Sicherheitslevels, welche die ZyWALL 10W unterstützt:

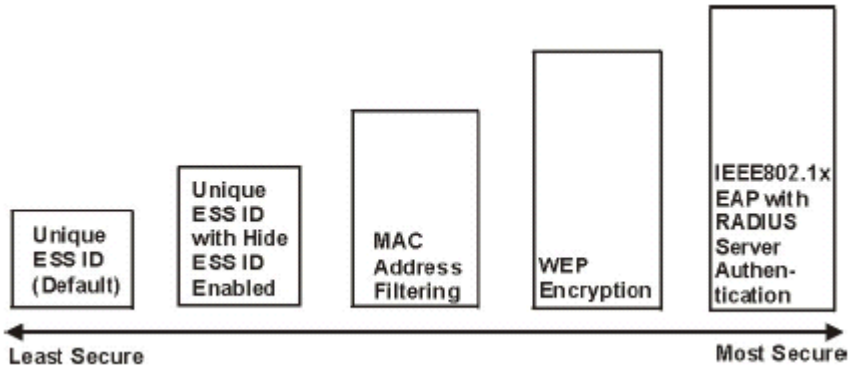


Abbildung 8: ZyWALL 10W – Wireless-Sicherheitslevels

Fazit Wireless-LAN

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen 😐

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☹

⊕

- Wireless-Clients können auf das Internet und interne Arbeitsstationen zugreifen, ohne dass ein zusätzlicher WLAN-Accesspoint angeschafft werden muss

⊖

- Die WLAN-Funktion konnte nur mit einer ZyXEL-eigenen WLAN-PCMCIA-Karte aktiviert werden
- Die Netzwerk-Authentisierung mit der Benutzerverwaltung direkt auf der Firewall konnte nicht er-

[22] Odyssey-Client, siehe http://www.funk.com/radius/wlan/wlan_c_radius.asp
[23] Quelle: ZyXEL Communications Corporation, vgl. ZyWALL 10/10W/50/100 User's Guide, Dez. 2002, Kapitel 7-1, Seite 99

⊕

- Sicherheitsfunktionen, wie das Verstecken der ESSID, der Einsatz von WEP-Verschlüsselung und MAC-Filter und die Netzwerk-Authentisierung mittels RADIUS sind implementiert

⊖

folgreich in Betrieb genommen werden

- WLAN-Systeme erhalten eine IP-Adresse vom gleichen DHCP-Server wie die übrigen internen Systeme. WLAN-Benutzer befinden sich somit direkt hinter der Firewall im internen Netzwerk; der Firewallschutz greift hier nicht
- Durch die inhärenten Schwächen, welche die gegenwärtigen Schutzmechanismen von WLANs aufweisen, stellt der Einsatz eines WLAN-Accesspoints direkt auf der Firewall ein gewisses Risiko dar

5.3.9 Virtual Private Network (VPN)

Die ZyWALL 10W ist mit VPN basierend auf IPSec (Internet Protocol Security) ausgestattet. Dabei werden sowohl das ESP-Protokoll (Encapsulating Security Payload) mit den kryptographischen Algorithmen DES und 3DES für die Vertraulichkeit und HMAC-MD5 und HMAC-SHA-1 für die Authentizität der Daten als auch das AH-Protokoll (Authentication Header) mit den kryptographischen Algorithmen HMAC-MD5 und HMAC-SHA-1 für die Authentizität der Daten unterstützt. Ausserdem kann der Firewall-Administrator zwischen dem Transport- und Tunnel-Modus wählen (siehe Abbildung 9).

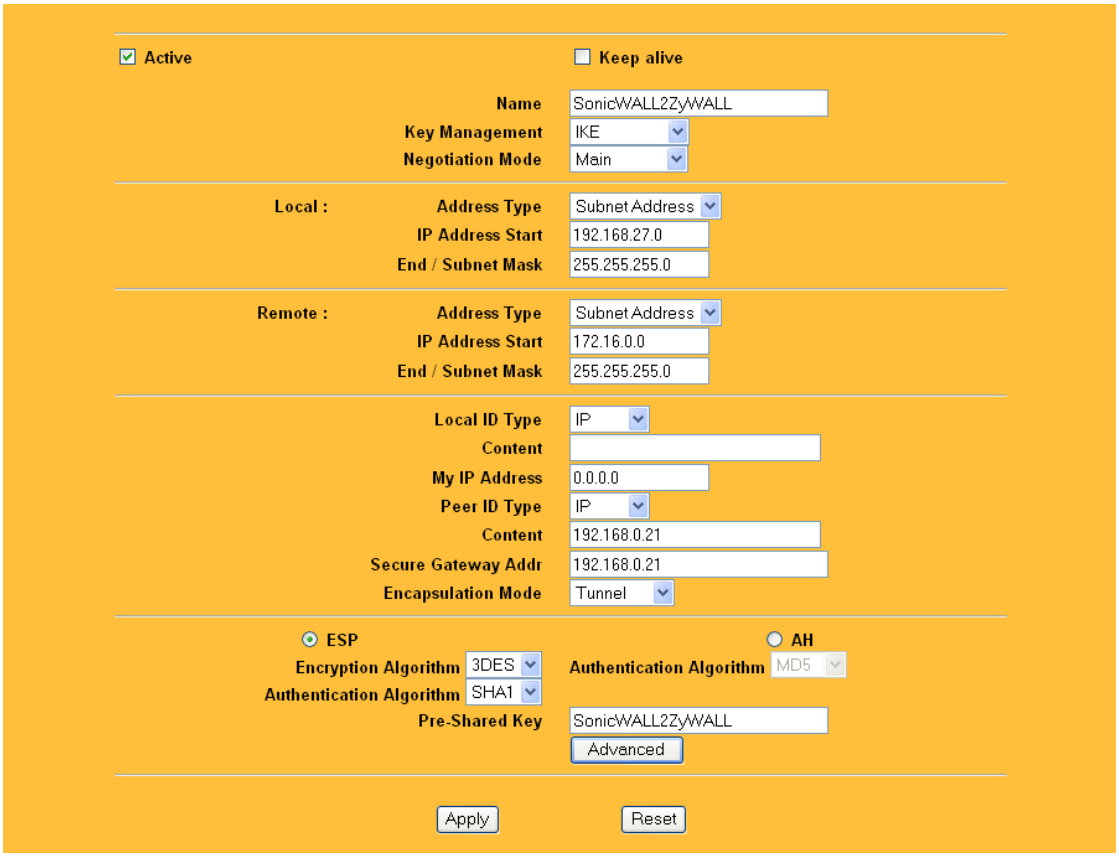


Abbildung 9: ZyWALL 10W – VPN-Grundeinstellungen

Das Schlüsselmanagement kann manuell oder basierend auf dem IKE-Protokoll (Internet Key Exchange) erfolgen. Beim IKE-Protokoll können für die beiden Phasen der Schlüsselaushandlung individuelle Einstellungen betreffend der zu verwendenden Algorithmen und der Schlüsselstärke vorgenommen werden (siehe Abbildung 10).

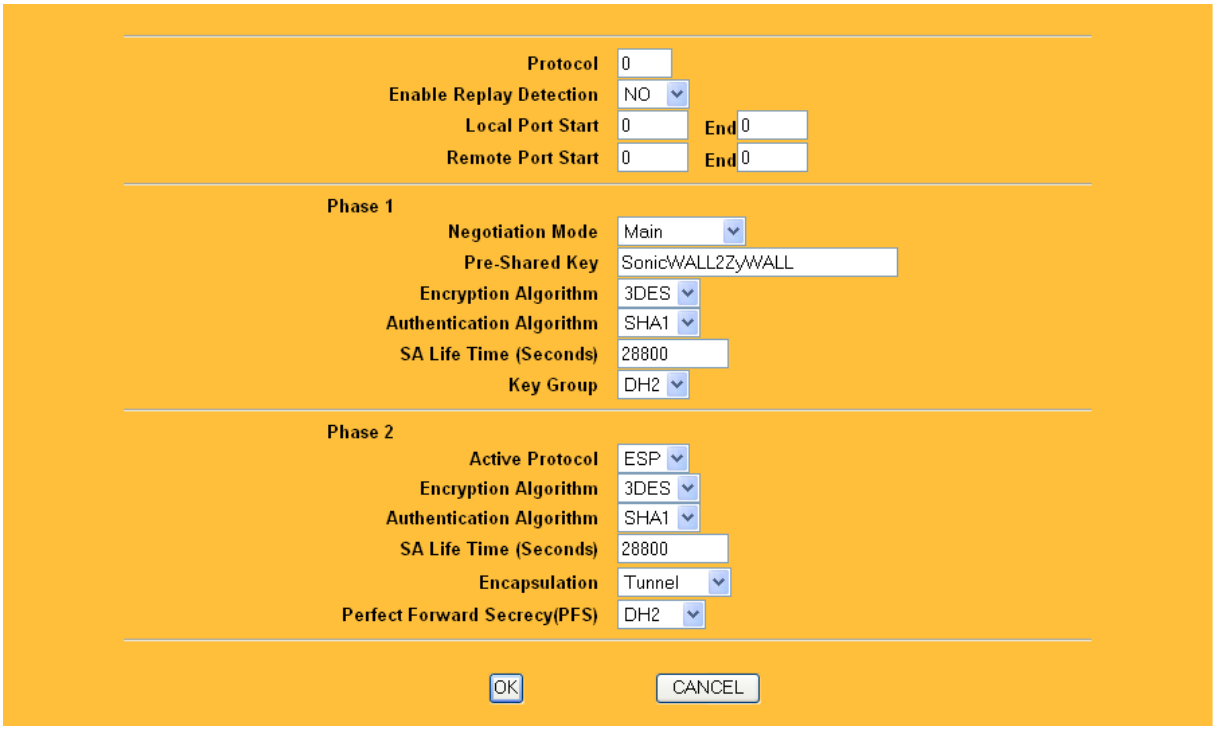


Abbildung 10: ZyWALL 10W – Einstellungen IKE Schlüsselaushandlung

Die Tests bezüglich VPN-Interoperabilität zwischen der ZyWALL 10W und der SonicWALL SOHO3 (siehe auch Kapitel 6.3.10) und zwischen der ZyWALL 10W und der Check Point Firewall-1 NG (siehe auch Kapitel 7.3.7) verliefen erfolgreich. Sowohl der VPN-Verbindungsaufbau zwischen der ZyWALL 10W und der SonicWALL SOHO3 als auch zwischen der ZyWALL 10W und der Check Point Firewall-1 NG klappte, sogar mit den höchsten Sicherheitseinstellungen, ohne Probleme. Die dabei verwendeten VPN-Einstellungen und die zugrunde liegenden Konfigurationen der verschiedenen Firewalls sind im Anhang, in den Kapiteln 13.2.2, 13.2.3 und 13.2.4 ersichtlich.

Um die Tests zwischen der ZyWALL 10W und der SonicWALL SOHO3 durchzuführen, wurde folgende Versuchsumgebung aufgebaut:

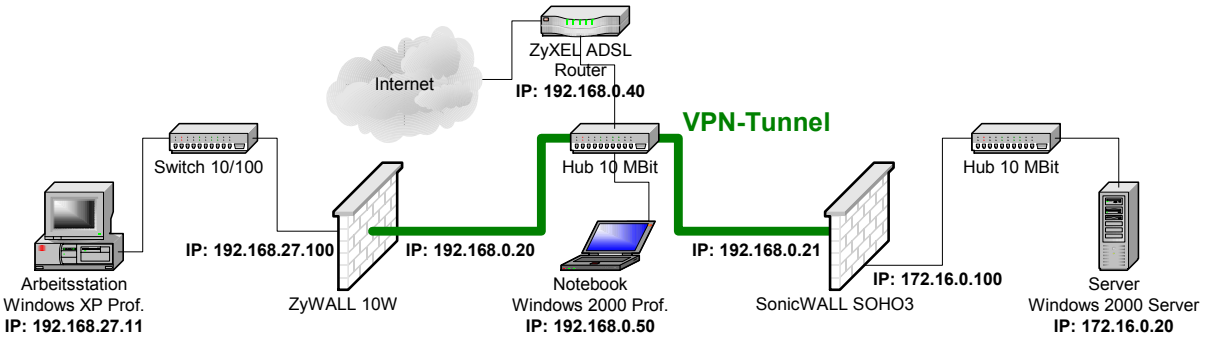


Abbildung 11: ZyWALL 10W – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der SonicWALL SOHO3

Die Aufzeichnung des Datenverkehrs mit einem Sniffer (installiert auf dem Notebook, IP-Adresse 192.168.0.50) zwischen den beiden Endsystemen 192.168.27.11 und 172.16.0.20 zeigt die Vereinbarung der „Security Association“ (Protokoll ISAKMP, Phasen 1 und 2) und die Übermittlung der verschlüsselten Daten (Protokoll ESP):

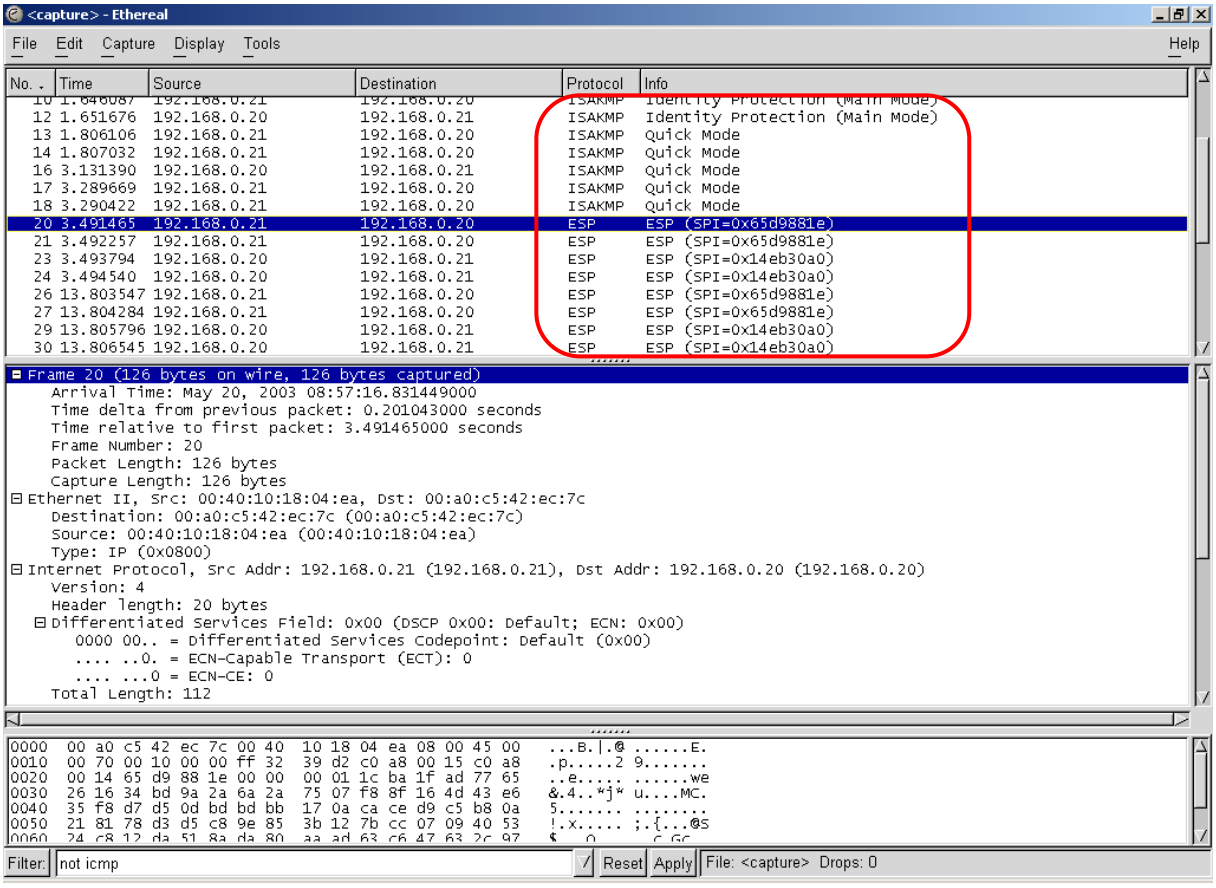

<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
12 1.651676 192.168.0.20 192.168.0.21 ISAKMP Identity Protection (Main Mode)
13 1.806106 192.168.0.21 192.168.0.20 ISAKMP Quick Mode
14 1.807032 192.168.0.21 192.168.0.20 ISAKMP Quick Mode
16 3.131390 192.168.0.20 192.168.0.21 ISAKMP Quick Mode
17 3.289669 192.168.0.21 192.168.0.20 ISAKMP Quick Mode
18 3.290422 192.168.0.21 192.168.0.20 ISAKMP Quick Mode
20 3.491465 192.168.0.21 192.168.0.20 ESP ESP (SPI=0x65d9881e)
21 3.492257 192.168.0.21 192.168.0.20 ESP ESP (SPI=0x65d9881e)
23 3.493794 192.168.0.20 192.168.0.21 ESP ESP (SPI=0x14eb30a0)
24 3.494540 192.168.0.20 192.168.0.21 ESP ESP (SPI=0x14eb30a0)
26 13.803547 192.168.0.21 192.168.0.20 ESP ESP (SPI=0x65d9881e)
27 13.804284 192.168.0.21 192.168.0.20 ESP ESP (SPI=0x65d9881e)
29 13.805796 192.168.0.20 192.168.0.21 ESP ESP (SPI=0x14eb30a0)
30 13.806545 192.168.0.20 192.168.0.21 ESP ESP (SPI=0x14eb30a0)
Frame 20 (126 bytes on wire, 126 bytes captured)
Arrival Time: May 20, 2003 08:57:16.831449000
Time delta from previous packet: 0.201043000 seconds
Time relative to first packet: 3.491465000 seconds
Frame Number: 20
Packet Length: 126 bytes
Capture Length: 126 bytes
Ethernet II, Src: 00:40:10:18:04:ea, Dst: 00:a0:c5:42:ec:7c
Destination: 00:a0:c5:42:ec:7c (00:a0:c5:42:ec:7c)
Source: 00:40:10:18:04:ea (00:40:10:18:04:ea)
Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.0.21 (192.168.0.21), Dst Addr: 192.168.0.20 (192.168.0.20)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
....0 = ECN-CE: 0
Total Length: 112
0000 00 a0 c5 42 ec 7c 00 40 10 18 04 ea 08 00 45 00 ...B.|.@ ......E.
0010 00 70 00 10 00 00 ff 32 39 d2 c0 a8 00 15 c0 a8 .p.....2 9.......
0020 00 14 65 d9 88 1e 00 00 00 01 1c ba 1f ad 77 65 ..e..... ......we
0030 26 16 34 bd 9a 2a 6a 2a 75 07 f8 8f 16 4d 43 e6 &.4..*j* u....MC.
0040 35 f8 d7 d5 0d bd bd bb 17 0a ca ce d9 c5 b8 0a 5....... ....
0050 21 81 78 d3 d5 c8 9e 85 3b 12 7b cc 07 09 40 53 !.x..... ;.{...@S
Filter: not icmp Reset Apply File: <capture> Drops: 0

Abbildung 12: ZyWALL 10W – Sniffer-Output des verschlüsselten Datenverkehrs zwischen der ZyWALL 10W und der SonicWALL SOHO3

Die VPN-Tests zwischen der ZyWALL 10W und der Check Point Firewall-1 NG basierten auf folgender Versuchsumgebung:

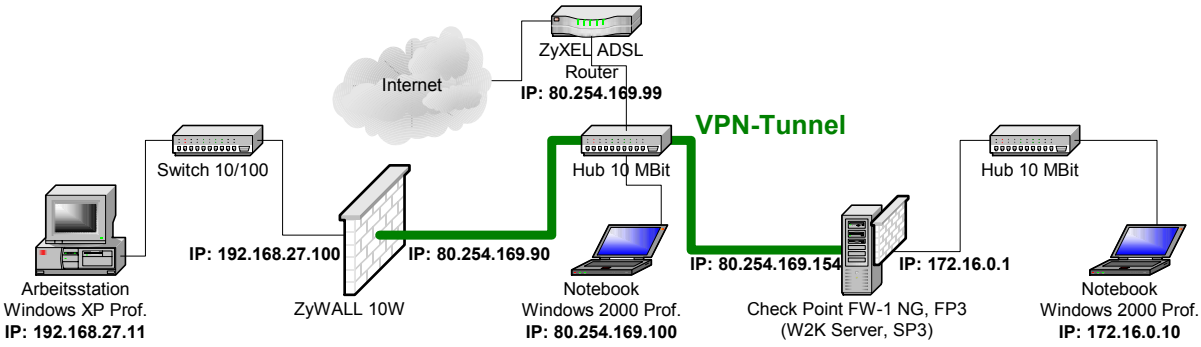


Abbildung 13: ZyWALL 10W – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der Check Point Firewall-1 NG

In einem nächsten Schritt wurde versucht, mit einem auf dem Notebook installierten VPN-Client eine VPN-Verbindung auf die Firewall aufzubauen. Da ZyXEL zu Ihrer Firewall keinen entsprechenden VPN-Client ausliefert, Microsoft ab Windows 2000 jedoch IPSec implementiert hat, lag der Versuch nahe, den VPN-Client mit Windows 2000 selber „herzustellen“. Etliche Mausklicks und Einstellungen später war dieser einsatzbereit und es konnte eine VPN-Verbindung auf die Firewall hergestellt werden. Da die Konfiguration des VPN-Clients unter Windows 2000 relativ komplex ist, befindet sich im Anhang unter Kapitel 13.2.5 eine Schritt-für-Schritt-Anleitung.

Es gilt jedoch festzuhalten, dass es nicht gelang, diese Verbindung mit den höchsten Sicherheitseinstellungen herzustellen. In der Phase 1 der Schlüsselaushandlung konnte der 3DES-Verschlüsselungsalgorithmus nicht eingesetzt werden (es musste DES verwendet werden), da sonst keine Verbindung aufgebaut werden konnte. Solche Probleme traten beim gleichen Versuch mit der SonicWALL-Firewall (siehe Kapitel 6.3.10) oder der Check Point Firewall (siehe Kapitel 7.3.7) jedoch nicht auf, was auf einen „Fehler“ in der Firmware der ZyWALL 10W hindeutet. Es ist ausserdem aufgefallen, dass kleinste Veränderungen an der Konfiguration des ZyWALL-VPN-Profils für den VPN-Clientzugriff (z.B. lediglich eine Änderung des Profilnamens) dazu führten, dass gar keine VPN-Verbindungen mehr aufgebaut werden konnte. Nach einigen Tests stand fest, dass entweder das Profil auf der Firewall komplett gelöscht und neu erstellt werden muss oder aber auf dem Notebook beim VPN-Client die VPN-Einstellungen auf der Netzwerkkarte zu deaktivieren und wieder zu aktivieren sind. Diese Probleme traten nur bei Änderungen am VPN-Client-Profil auf; Änderungen an den Profilen für die VPN-zu-VPN-Verbindungen zwischen der ZyWALL und den beiden anderen Firewalls konnten hingegen problemlos durchgeführt werden. Die hier geschilderten Instabilitäten traten ebenfalls nur mit der ZyWALL, jedoch nicht mit der SonicWALL oder der Check Point Firewall auf. Die aktuelle Firmware der ZyWALL 10W scheint deshalb im Bereich der VPN-Unterstützung noch nicht ganz ausgereift zu sein.

Fazit VPN

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen 😐

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

- Sichere (verschlüsselte) Netzwerkverbindungen mit anderen VPN-Gateways (z.B. anderen Firewalls) und zwischen VPN-Clients und Firewall möglich
- Interoperabilität mit anderen Firewalls
- Als VPN-Client kann Windows 2000 (oder höher) mit IPSec verwendet werden; keine Anschaffung eines dedizierten VPN-Clients nötig

- Instabilitäten der VPN-Funktion, je nach Einstellungen und Anbindung

5.3.10 Diagnosemöglichkeiten

Im Rahmen der Diagnosemöglichkeiten stehen mittels Telnet oder direkt über den Konsolen-Port einige wenige Werkzeuge zur Verfügung. So kann der aktuelle Systemstatus inkl. der Status der Interface angezeigt werden. Das Internet-Setup zum ISP lässt sich direkt durch die Firewall testen, die IP-Adresse auf dem externen Interface kann bei Einsatz von DHCP gelöst und neu gebunden werden und es besteht die Möglichkeit, die Firewall neu zu booten. Ausserdem kann der Firewall-Administrator direkt auf die Command-Shell der Firewall zugreifen, auf welcher ihm viele weitere Befehle und Analysemöglichkeiten zur Verfügung stehen.

Fazit Diagnosemöglichkeiten

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen	☺
Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs	-

- Es stehen einige Diagnose-Werkzeuge zur Verfügung
- Zugriff auf die Command-Shell der Firewall möglich (zur Durchführung weiterer Diagnosen bzw. Tests)

5.3.11 Remote-Management

Das Remote-Management kann bei der ZyWALL 10W mittels Telnet, FTP, WWW (HTTP) und SNMP erfolgen. Standardmässig sind alle Protokolle auf der Firewall aktiviert und der Zugriff ist grundsätzlich sowohl über das interne als auch das externe Interface der Firewall von jedem PC aus gestattet. Um über das externe Interface zugreifen zu können, müssen jedoch zuerst (glücklicherweise) noch entsprechende Firewall-Regeln definiert werden. Jedes der Managementprotokolle kann deaktiviert werden oder der Zugriff lässt sich dahingehend anpassen, dass entweder nur über das interne oder nur über das externe Interface eine Verbindung mit diesem Protokoll hergestellt werden darf. Zudem lässt sich der erlaubte Zugriff auf genau eine IP-Adresse einschränken.

Analysen mit einem Sniffer haben bezüglich der Administrator-Passwortübermittlung im Netzwerk folgendes Ergebnis geliefert: Die Übermittlung des Firewall-Administratorpassworts über das Netzwerk erfolgt beim Management-Zugriff mittels Telnet- und FTP-Protokoll wie zu

erwaten war in Klartext. Nur beim Management-Zugriff über das HTTP-Protokoll wird das Passwort nicht in Klartext, sondern als MD5-Hashwert transferiert.

Beim SNMP-Protokoll wird der standardmässige Community-String „public“ verwendet. Dieser lässt sich jedoch problemlos ändern.

Im Bereich „Remote Management“ kann auch noch definiert werden, wie die Firewall auf „Pings“ reagieren soll. Standardmässig lässt sie ein „Ping“ sowohl auf das interne als auch auf das externe Interface zu (um das externe Interface anpingen zu können, braucht es jedoch wiederum zuerst eine entsprechende Firewall-Regel). Zudem kann die Option aktiviert werden, dass die Firewall Anfragen auf unbenutzte Ports (wie sie z.B. beim Portscanning erfolgen) nicht beantworten soll (so genannter „Stealth-Modus“ der Firewall).

Eine Portscanning-Analyse unter Mithilfe eines Sniffers führte dabei zu folgenden Resultaten:

Durchgeführter Test	*Firewall-Interface*	*Stealth-Modus aktiv?*	*Von der Firewall erhaltene Resultate*
Portscan aus dem WAN gegen die Firewall auf nicht verwendete Ports	Extern	Nein	Keine Antwort von der Firewall / Ports werden vom Portscanner als „gefiltert“ bezeichnet
Portscan aus dem WAN gegen die Firewall auf nicht verwendete Ports	Extern	Ja	Keine Antwort von der Firewall / Ports werden vom Portscanner als „gefiltert“ bezeichnet
Portscan aus dem LAN gegen die Firewall auf nicht verwendete Ports	Intern	Nein	Firewall antwortet mit einem Reset- und Acknowledgment-Paket (RST/ACK) / Ports werden vom Portscanner als „geschlossen“ bezeichnet
Portscan aus dem LAN gegen die Firewall auf nicht verwendete Ports	Intern	Ja	Firewall antwortet nur mit einem Reset-Paket (RST) / Ports werden vom Portscanner als „gefiltert“ bezeichnet

Tabelle 13: ZyWALL 10W – Resultate Portscans mit Firewall-Stealth-Modus

Es fällt auf, dass die Aktivierung des Stealth-Modus der Firewall bei Portscans aus dem WAN auf das externe Interface der Firewall keinen Einfluss auf die Resultate hat. Erst bei einem Portscan aus dem LAN auf das interne Interface der Firewall wird der Unterschied zwischen aktiviertem und deaktiviertem Stealth-Modus ersichtlich.

<u>Fazit Remote-Management</u>

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☹

⊕

- Mehrere Protokolle stehen für das Remote-Management zur Verfügung
- Obwohl der Remote-Management-Zugriff standardmässig auch über das externe Interface der Firewall gestattet ist, muss zuerst noch eine entsprechende Regel auf der Firewall erfasst und aktiviert werden

⊖

- Das SNMP-Protokoll weist den standardmässigen Community-String „public“ auf, welcher zuerst durch den Firewall-Administrator geändert werden muss. Dies stellt ein gewisses Sicherheitsrisiko dar
- Das Firewall-Administrator-Passwort wird beim Zugriff über das Telnet- und FTP-Protokoll in Klar-

- Jedes Remote-Management-Protokoll lässt sich aktivieren und deaktivieren
- Das Firewall-Administrator-Passwort wird beim Zugriff über das HTTP-Protokoll nicht in Klartext, sondern als MD5-Hashwert über das Netzwerk transferiert
- Der Zugriff mittels Remote-Management kann für eine einzelne IP-Adresse eingeschränkt werden
- Die Firewall lässt sich in den so genannten „Stealth Modus" setzen

text über das Netzwerk transferiert

- Der Datenverkehr des Remote-Managements wird bei keiner der angebotenen Varianten verschlüsselt

5.3.12 Firmware-Updates

Die Updates der Firewall-Firmware erfolgen manuell. Die jeweils aktuelle Firmware kann beim Hersteller heruntergeladen werden. Der Web-Konfigurator der Firewall verfügt über einen Menupunkt „Firmware Upload", über welchen die neue Firmware eingespielt werden kann. Natürlich ist ein Update auch direkt über die Konsole oder mittels FTP möglich.

Fazit Firmware-Updates

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

- Hersteller führt Fehlerkorrekturen durch und stellt die neue Firmware auf seiner Homepage zum Download zur Verfügung
- Download der aktuellen Firmware von der Hersteller-Homepage problemlos möglich
- Update lässt sich effizient und ohne Schwierigkeiten über einen entsprechenden Konfigurations-Menupunkt einspielen

5.3.13 Dial-Up-Backup

Der Konsolen-Port der Firewall lässt sich auch als serielle Dial-Up-Backup-Schnittstelle einsetzen (mit einem Schalter kann zwischen der Konsolen-Funktion und der Dial-Up-Backup-Funktion hin und her gewechselt werden). Falls das primäre WAN-Interface aussetzt, kann die Firewall automatisch auf die Dial-Up-Backup-Funktion ausweichen. Sobald das primäre WAN-Interface wieder verfügbar ist, wird die Backup-Verbindung abgebaut und der Verkehr fliesst wieder über die ursprüngliche WAN-Verbindung.

Fazit Dial-Up-Backup

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Im Problemfall kann mittels Dial-Up-Backup auf einen anderen Provider ausgewichen werden
- Die Ausweichmöglichkeit trägt zu einer höheren Gesamtverfügbarkeit der WAN-Verbindung und somit auch zu einer höheren Sicherheit bei (Verfügbarkeit als Sicherheitsziel)

⊖

5.3.14 Verkehrsumleitung

Für den Fall, dass die normale WAN-Verbindung ausfällt, besteht die Möglichkeit, eine alternative Route zu wählen. Dabei wird der Verkehr über ein anderes WAN-Gateway umgeleitet. Die Firewall kann in einem frei definierbaren Intervall überprüfen, ob die standardmässige WAN-Verbindung noch steht, indem ein Zielsystem auf der WAN-Seite angepingt wird. Falls keine Antwort mehr zurückkommt, wird der Verkehr über das alternative WAN-Gateway umgeleitet. Sobald die standardmässige Verbindung wieder steht, fliesst der Verkehr erneut über das ursprüngliche Gateway.

Fazit Verkehrsumleitung

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Bei einem Unterbruch des primären WAN-Verbindung kann der WAN-Zugang trotzdem aufrecht erhalten werden; dadurch wird die Verfügbarkeit des WAN-Zugangs erhöht.

⊖

5.3.15 Backup und Restore der Firewall-Konfiguration

Die Firewall-Konfiguration (inkl. aller Einstellungen zu den Zusatzfunktionalitäten) lässt sich mittels HTTP (Web-GUI), Telnet, FTP oder über den Konsolen-Port sichern und bei Bedarf wiederherstellen. Ausserdem kann die Firewall auf ihre Werkeinstellungen zurückgesetzt werden.

Fazit Backup und Restore der Firewall-Konfiguration

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Alle Einstellungen lassen sich in einer Backup-Datei sichern, welche bei Bedarf ohne Probleme wieder zurückgespielt werden kann
- Backup und Restore können über alle Remote-Management-Varianten durchgeführt werden

⊖

5.3.16 Logische Netzwerksegmente

Die Firewall unterstützt über ihr physisches LAN-Interface bis zu drei logische LAN-Interface und somit auch bis zu drei logische Netzwerksegmente. Der Verkehr zwischen den logischen LAN-Segmenten passiert somit die Firewall (diese nimmt natürlich zwingend auch das Routing vor), obschon die Geräte unter Umständen am gleichen Hub oder Switch angeschlossen sind. Auf der Firewall können Regeln definiert werden, um den Verkehr zwischen den logischen LAN-Segmenten einzuschränken.

Fazit logische Netzwerksegmente

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Das interne Netzwerk (LAN) kann auf einfache Art und Weise segmentiert werden
- Firewall-Regeln können zwischen den logischen Segmenten konfiguriert werden, wodurch sich der Verkehr gezielt kontrollieren lässt
- Es lässt sich auf diese Weise eine (logische) DMZ aufbauen

⊖

- Obschon der Verkehr zwischen den logischen Netzwerksegmenten durch Firewall-Regeln eingeschränkt werden kann, bietet diese Variante nicht den gleichen Schutz wie eine physische Trennung (z.B. mittels dediziertem DMZ-Port)

5.3.17 WAN-Protokolle

Die Firewall unterstützt mittels PPPoE (Point-to-Point Protocol over Ethernet) eine direkte Verbindung zu einem Breitbandmodem (z.B. für eine Anbindung an einen ADSL-ISP). Dabei können die Zugangsdaten (Benutzername, Passwort) für den ISP direkt auf der Firewall eingegeben und gespeichert werden. Ausserdem lässt sich einstellen, dass die Verbindung zum ISP durch diesen nicht „unterbrochen“ werden kann („Nailed Up Connection“). Einige ISP unterbrechen eine Breitbandverbindung nach einer gewissen Zeit, um ein „always-on“ der Kunden zu unterbinden. Mit der Funktion „Nailed Up Connection“ wird diesem Umstand entgegengewirkt und der Kunde bleibt permanent mit dem ISP verbunden.

Zudem wird das PPTP (Point-to-Point Tunneling Protocol) für eine Anbindung an einen ISP unterstützt. Auf diese Weise lässt sich ein verschlüsselter VPN-Zugang zum ISP einrichten.

Fazit WAN-Protokolle

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs -

⊕

- Die Benutzerinformationen für einen Internet-Breitbandzugang wie z.B. ADSL lassen sich direkt auf der Firewall hinterlegen
- Die Verbindung zu einem ISP kann permanent aufrecht erhalten werden
- Mit dem Protokoll PPTP kann ein verschlüsselter Provider-Zugang, falls vom Provider unterstützt, hergestellt werden

⊖

6. SONICWALL SOHO3 25-USER MIT VPN

6.1 Allgemeine Hinweise zur Firewall

Bei dieser Firewall handelt es sich ebenfalls um ein Produkt, welches auf den KMU-Markt (SOHO-Markt) abzielt. Innerhalb der SonicWALL-Firewall-Produktfamilie ist das Modell SonicWALL SOHO3 am Ende des unteren Drittels der Produkte anzusiedeln.[24]

Die Firewall arbeitet ebenfalls nach dem „Stateful Inspection"-Prinzip. Auch dieses Modell verfügt über zwei Interface – ein internes Interface und ein externes Interface; ein so genannter DMZ-Port (drittes Interface) ist nicht vorhanden. Mit der aktuellen Lizenz können bis zu 25 Benutzer (IP-Adressen) eine Verbindung vom internen Netzwerk ins externe Netzwerk gleichzeitig herstellen. Weitere Verbindungen werden nach dem Erreichen dieses Schwellenwerts nicht mehr zugelassen.

Die Administration erfolgt grundsätzlich „remote" über die Protokolle HTTP oder HTTPS (SSL). Die Firewall verfügt zwar über ein „Command Line Interface" (CLI ⇨ eine Art Konsolen-Port), dessen Funktionalität jedoch stark eingeschränkt ist. Die Verbindung kann entweder mittels Nullmodem-Kabel von einem Computer aus oder über einen Modemzugang (unterstützt werden gemäss Hersteller[25] jedoch nur US Robotics V.90 / V.92 Modems) hergestellt werden. Die nach einer Verbindung über den CLI-Port zur Verfügung stehenden Befehle beschränken sich mehr oder weniger auf Status-Informationen der Firewall und auf das Sichern (Backup) oder Wiederherstellen (Restore) der Firewall-Konfiguration.

Die während dieser Diplomarbeit gewonnen Erkenntnisse zu den Zusatzfunktionalitäten der SonicWALL SOHO3 Firewall basieren alle auf der zu diesem Zeitpunkt aktuellen Firmware 6.4.2.0.

Zum Testen der Firewall-Zusatzfunktionalitäten wurde folgende Versuchsumgebung aufgebaut:

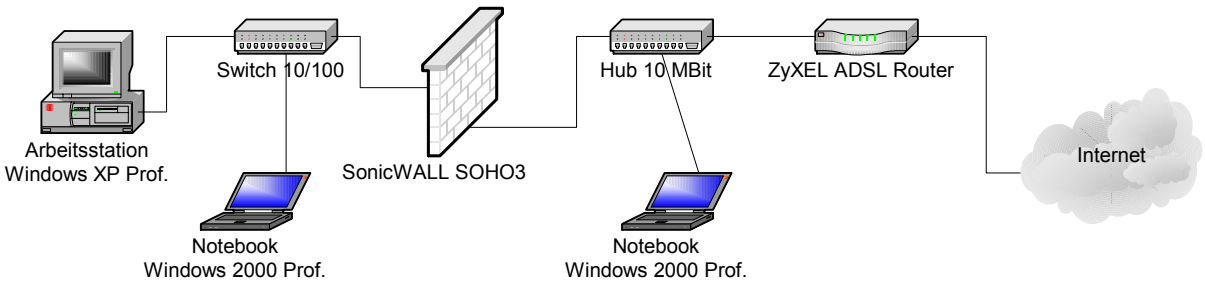


Abbildung 14: SonicWALL SOHO3 – Versuchsumgebung für die Durchführung der Firewall-Tests

Die Windows XP Arbeitsstation und das Windows 2000 Notebook waren mit diversen Tools (Portscanner, Sniffer usw.) ausgestattet, um die technischen Tests möglichst umfassend

[24] SonicWALL-Firewall-Produkteübersicht, siehe http://www.sonicwall.com/products/vpnapp.html
[25] vgl. SonicWALL – Internet Security Applicances, Rev. A 10/01, Seite 30

durchführen zu können. Das Notebook konnte wahlweise entweder hinter der Firewall am Switch oder vor der Firewall am Hub angeschlossen werden.

6.2 Grundkonfiguration und wesentliche Standardeinstellungen

Die Grundkonfiguration der Firewall erfolgt mittels HTTP- oder HTTPS-Protokoll (Web-Konfigurationsoberfläche) über das interne Interface der Firewall. Die Firewall ist standardmässig auf die IP-Adresse 192.168.168.168 konfiguriert, der Anmeldebenutzername lautet „admin“ und das Standard-Passwort ist „password“. Nach dem erstmaligen Anmelden erscheint sofort ein Konfigurations-Wizard; dieser kann jedoch auch abgebrochen und zu einem späteren Zeitpunkt erneut gestartet werden. Falls der Firewall-Administrator den Wizard Schritt für Schritt durchgeht, kann er auf diese Weise folgende Einstellungen auf der Firewall vornehmen:

- Neues Passwort setzen
- Zeitzone auswählen
- Art des Internet-/WAN-Zugriffs festlegen (statische IP-Adresse, dynamische IP-Adresse, PPTP usw.)
- Eingabe der IP-Adresse des externen Interface bei Verwendung einer statischen IP-Adresse
- Eingabe der DNS-Server
- Eingabe der IP-Adresse des internen Interface
- Aktivierung oder Deaktivierung des DHCP-Servers auf der Firewall mit der Eingabe der entsprechenden Parameter

Falls der Konfigurations-Wizard abgebrochen wird, weist die Firewall nach der ersten Inbetriebnahme folgende Einstellungen auf:

- Firewall ist nicht aktiv, da die Netzwerkeinstellungen auf dem externen Interface noch nicht vorgenommen wurden
- Vom LAN ins WAN ist aller Verkehr erlaubt
- Vom WAN ins LAN ist aller Verkehr verboten
- Vom LAN auf die Firewall (internes Interface) ist HTTP (TCP-Port 80) und HTTPS (TCP-Port 443) erlaubt
- Internes Interface:
  - IP-Adresse 192.168.168.168 / 255.255.255.0
- Time-Server (interne NTP-Serverliste der SonicWALL) mit GMT-8:00-Zeitzone aktiviert
- Remote Management
  - WWW mittels HTTP (TCP-Port 80), alle IP-Adressen aus LAN-Segment zugelassen
  - WWW mittels HTTPS (TCP-Port 443), alle IP-Adressen aus LAN-Segment zugelassen
- Logging ist aktiviert für: System Maintenance, System Errors, Blocked Web Sites, Blocked Java etc., User Activity, Attacks, Dropped TCP, Dropped UDP, Dropped ICMP
- Alarmierung ist aktiviert für: Attacks und System Errors
- Log-File wird überschrieben, sobald es voll ist

Bevor die Firewall im Betrieb umfassend eingesetzt werden kann, muss sie zuerst einmal beim Hersteller über das Internet registriert werden. Die ganze Registrationsprozedur erweist sich als ziemlich mühsam. Es gilt viele Fragen zu beantworten, welche zum Teil offensichtlich aus Marketinggründen gestellt werden. Erst nach der Registration hat der Firewall-Administrator die Möglichkeit, die aktuelle Firmware zu seiner Firewall herunterzuladen und

einige der (bereits bezahlten) Zusatzfunktionalitäten (wie z.B. das VPN-Modul) freizuschalten.

Fazit Grundkonfiguration und wesentliche Standardeinstellungen

Beurteilung der Grundkonfiguration bezüglich Aufwand, Verständlichkeit usw.

Auswirkungen der Grundkonfiguration auf die Gesamtsicherheit der Firewall

- Wesentliche Einstellungen können mit Hilfe eines Konfigurations-Wizards durchgeführt werden
- Aufforderung zum Wechsel des Standardpasswortes bei Konfiguration mittels Wizard
- Gesamter Verkehr vom WAN ins LAN wird standardmässig geblockt
- „Intrusion Detection"-Funktionen sind aktiviert
- Logging ist aktiviert

- Kein Konsolen-Port zur umfassenden Konfiguration vorhanden
- Registrationsprozedur beim Hersteller ziemlich mühsam

6.3 Zusatzfunktionalitäten

Die Zusatzfunktionalitäten werden im folgenden Kapitel grundsätzlich in der gleichen Reihenfolge, in der sie in Kapitel 2 generisch umschrieben wurden, abgehandelt. Falls die Firewall eine der in Kapitel 2 erwähnten Zusatzfunktionalitäten nicht unterstützt, wird diese in diesem Kapitel auch nicht aufgeführt (es erfolgt somit kein expliziter Hinweis, dass die entsprechende Funktionalität nicht zur Verfügung steht; eine solche Gesamtübersicht folgt in Kapitel 8).

Es gilt zudem zu berücksichtigen, dass die Konfiguration einiger in Kapitel 2 erwähnten Zusatzfunktionalitäten auf der Firewall jeweils an ein und derselben Stelle bzw. im gleichen Menu erfolgt. In einem solchen Fall werden diese Zusatzfunktionalitäten auch im vorliegenden Kapitel entsprechend zusammengefasst.

Am Schluss dieses Kapitels (ab Kapitel 6.3.16) werden noch weitere interessante Eigenschaften der Firewall, welche jedoch in Kapitel 2 keine Berücksichtigung als eigenständige Zusatzfunktionalitäten fanden (es handelt sich dabei mehr um willkommene Eigenschaften als um echte Zusatzfunktionalitäten), in gleicher Art und Weise wie die übrigen Zusatzfunktionalitäten umschrieben.

6.3.1 Authentisierungsmöglichkeiten

Die Firewall verfügt über eine eigene Benutzerverwaltung, in welcher bis zu 100 Benutzer erfasst werden können. Falls ein RADIUS-Server zur Verfügung steht, kann auch dieser für die Benutzerauthentisierung verwendet werden, da die Firewall eine entsprechende Schnittstelle anbietet. Wenn mehr als 100 Benutzer verwaltet werden sollen, ist zwingend ein RADIUS-Server nötig.

Ein authentisierter Benutzer kann über Berechtigungen in den Bereichen „Remote Access“ (Zugriff auf LAN-Ressourcen aus dem WAN/Internet), „Bypass Filter“ (Content- und URL-Filter kommen nicht zur Anwendung) und „Limited Management Capabilities“ (für limitierten lokalen Firewall-Management-Zugriff) verfügen. Diese Rechte lassen sich pro Benutzer einzeln vergeben.

Die Benutzer authentisieren sich mittels Benutzernamen und Passwort. Um das Risiko vor allfälligen Brute-Force-Attacken auf die Benutzerkonten zu reduzieren, kann definiert werden, nach wie vielen Login-Fehlversuchen (Anzahl Fehlversuche innerhalb einer Minute von der gleichen IP-Adresse aus) das Benutzerkonto für welche Zeitdauer gesperrt werden soll.

Fazit Authentisierungsmöglichkeiten

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Ein Benutzer erhält erst Zugriff auf einzelne Bereiche oder Funktionen nachdem er sich erfolgreich authentisiert hat
- Gezielte Freigaben für Zugriffe aus dem WAN aufs LAN und aus dem LAN aufs WAN möglich
- Mehrere Personen können autorisiert werden, eingeschränkte Firewall-Management-Aktivitäten (Abruf von Status-Informationen, Zugriff auf Log-Datei, Neustart der Firewall usw.) durchzuführen

⊖

6.3.2 Zeiteinschränkung einzelner Firewall-Regeln

Die Firewall-Regeln lassen sich sowohl bezüglich Tageszeit als auch bezüglich Wochentag einschränken (siehe Abbildung 15).

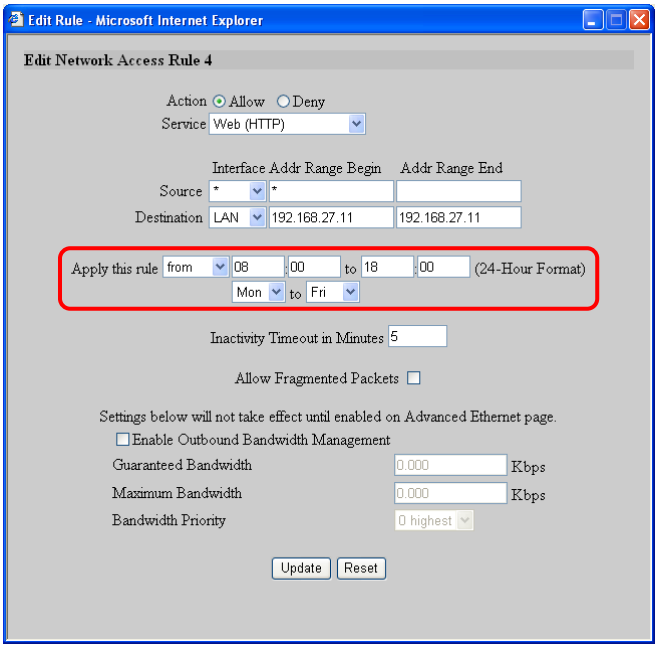

Edit Rule - Microsoft Internet Explorer
Edit Network Access Rule 4
Action Allow Deny
Service Web (HTTP)
Interface Addr Range Begin Addr Range End
Source * *
Destination LAN 192.168.27.11 192.168.27.11
Apply this rule from 08 :00 to 18 :00 (24-Hour Format)
Mon to Fri
Inactivity Timeout in Minutes 5
Allow Fragmented Packets
Settings below will not take effect until enabled on Advanced Ethernet page.
Enable Outbound Bandwidth Management
Guaranteed Bandwidth 0.000 Kbps
Maximum Bandwidth 0.000 Kbps
Bandwidth Priority 0 highest
Update Reset

Abbildung 15: SonicWALL SOHO3 – Zeiteinschränkung der Firewall-Regeln

Auf diese Weise können Firewall-Regeln erstellt werden, welche z.B. nur während der Geschäftszeiten oder nur während der Nacht aktiv sein sollen.

Fazit Zeiteinschränkungen einzelner Firewall-Regeln

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕ ⊖

- Firewall-Regeln können zeitlich beliebig eingeschränkt werden; auf diese Weise können bestimmte Aktivitäten (z.B. Wartungszugriffe, externe Partner-Zugriffe usw.) gezielt gesteuert und dadurch besser überwacht und kontrolliert werden

6.3.3 Content- und URL-Filtering

SonicWALL fasst unter dem Betriff „Filter“ sowohl das Content-Filtering, als auch das URL-Filtering/-Blocking zusammen (siehe Kapitel 2.3 und 2.4 bezüglich der Definition dieser Begriffe, wie sie in dieser Arbeit verwendet werden). Der Firewall-Administrator kann festlegen, ob das URL-Filtering durch die SonicWALL selber oder aber durch einen Dritthersteller von URL-Filtering-Software (SonicWALL bietet Schnittstellen zu N2H2 von WorkGroup Solutions[26] und Websense Enterprise von Websense Inc.[27]) vorgenommen werden soll. Das Con-

[26] WorkGroup Solutions – N2H2 Filter, siehe http://www.n2h2filter.com/
[27] Websense Inc., siehe http://www.websense.com/

tent-Filtering ist davon nicht betroffen und wird in jedem Fall von der SonicWALL-Firewall durchgeführt.

Unter dem Begriff „Restrict Web Features“ lassen sich auf der Firewall ActiveX-Controls, Java-Applets (ohne JavaScript), Cookies, Web-Proxies und bekannte gefälschte digitale Zertifikate filtern (Content-Filtering). Die nachfolgende Tabelle zeigt die diesbezüglich durchgeführten Tests und deren Ergebnisse auf:

Getestete Funktion	***Durchgeführte Tests***	***Ergebnisse / Erkenntnisse***	
ActiveX-Filter	➢ ActiveX-Filter in der Firewall aktiviert ➢ Konkrete Tests mit ActiveX-Controls auf einer ActiveX-Demo-Website[28] (Websitezugriff mittels HTTP-Protokoll) Verwendeter Browser: Internet Explorer 6.0 ➢ Konkrete Tests mit ActiveX-Controls innerhalb des kostenpflichtigen Sicherheitsportals eSecurityOnline[29] (Reporting-Funktionen, welche auf ActiveX-Controls basieren ⇨ Websitezugriff mittels HTTPS-Protokoll) Verwendeter Browser: Internet Explorer 6.0	Die ActiveX-Controls auf der Demo-Website wurden durch die Firewall erfolgreich geblockt resp. das Herunterladen der Controls wurde verhindert. Das ActiveX-Control von eSecurityOnline konnte trotz aktiviertem ActiveX-Filter in der Firewall heruntergeladen und ausgeführt werden. Dieses Verhalten ist jedoch nachvollziehbar, da der ganze Netzwerkverkehr mittels SSL verschlüsselt wurde und die Firewall das ActiveX-Control deshalb nicht feststellen konnte. Fazit: Der ActiveX-Filter arbeitet grundsätzlich wie erwartet. Sobald der Website-Zugriff mittels SSL-Verschlüsselung erfolgt (HTTPS), können ActiveX-Controls jedoch trotz aktiviertem Filter heruntergeladen und ausgeführt werden.	✓
Java-Filter	➢ Java-Filter in der Firewall aktiviert ➢ Test der Java-Funktion mittels Heise-Browsercheck. Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a ➢ Test der Homepage des Autors[30], auf welcher die Navigationsleiste in Java programmiert wurde (normaler Internet-Zugriff mittels HTTP-Protokoll) Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a ➢ Test der Homepage des Autors auf einem eigenen Test-Server mit einem SSL-Serverzertifikat von Thawte[31] zu Evaluationszwecken (Websitezugriff mittels HTTPS-Protokoll) Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a	Die Java-Applets wurden sowohl auf der Heise-Browsercheck-Seite, als auch auf der Homepage des Autors beim Zugriff mittels HTTP-Protokoll nicht mehr angezeigt. Beim Zugriff mittels HTTPS-Protokoll auf die Homepage des Autors (eigener Testserver) wird das Java-Applet heruntergeladen und ausgeführt. Dieses Verhalten ist jedoch nachvollziehbar, da der ganze Netzwerkverkehr mittels SSL verschlüsselt wurde und die Firewall das Java-Applet deshalb nicht feststellen konnte. Fazit: Java-Applets werden bei den getesteten Browsern grundsätzlich korrekt geblockt. Sobald der Website-Zugriff mittels SSL-Verschlüsselung erfolgt (HTTPS), können die Java-Applets jedoch trotz aktiviertem Filter heruntergeladen und ausgeführt werden.	✓
Java-Filter	➢ Java-Filter in der Firewall aktiviert ➢ Test der Java-Funktion mittels Heise-Browsercheck. Verwendete Browser: Internet Explorer	Die Java-Applets wurden sowohl auf der Heise-Browsercheck-Seite, als auch auf der Homepage des Autors nicht mehr angezeigt. Fazit: Java-Applets werden bei den getes-	✓

[28] OCX-Tester, siehe http://www.ilook.fsnet.co.uk/vb/vbdemo.htm
[29] eSecurityOnline, siehe http://www.esecurityonline.com
[30] tomsplace, siehe http://www.tomsplace.ch
[31] Thawte, siehe http://www.thawte.com

Getestete Funktion	*Durchgeführte Tests*	*Ergebnisse / Erkenntnisse*	
	6.0 und Mozilla 1.2a ➢ Test der Homepage des Autors[32], auf welcher die Navigationsleiste in Java programmiert wurde. Verwendete Browser: Internet Explorer 6.0 und Mozilla 1.2a	teten Browsern korrekt geblockt.	
Cookie-Filter	➢ Cookie-Filter in Firewall aktiviert ➢ Aufruf folgender Homepages mit den Browsern Internet Explorer 5.5 und 6.0 und Mozilla 1.2a und 1.3a: ○ Swiss-Homepage, Login-Seite[33] ○ Amazon-Homepage[34] ○ Homepage des Autors Alle diese Homepages setzten im Normalfall beim Besuch der Homepage ein Cookie auf dem PC des Besuchers	Der Cookie-Filter verhält sich bei allen Browsern identisch: ➢ Die Swiss-Homepage kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben ➢ Die Amazon-Homepage kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben ➢ Homepage des Autors kann problemlos aufgerufen werden und das Cookie wird trotz aktivem Cookie-Filter geschrieben. Das Cookie kann beim nächsten Besuch auch wieder ohne Probleme ausgelesen werden Fazit: Der Cookie-Filter arbeitet nicht wie erwartet, die Cookies aller getesteten Webseiten werden trotz aktivem Filter auf den Benutzer-PCs gespeichert und auch wieder ausgelesen (Test mittels Homepage des Autors). Bei den getesteten Webseiten ist deshalb kein Unterschied im Verhalten bezüglich Cookies zwischen aktiviertem und deaktiviertem Cookie-Filter ersichtlich.	✘
Web-Proxy-Filter	➢ Web-Proxy-Filter in Firewall aktiviert ➢ Internet-Zugriffsversuche mit im Browser aktiven Proxy-Einstellungen eines externen Web-Proxies (Proxy-Server befindet sich im WAN). Tests sowohl mit dem Proxy-Server des eigenen ISPs (Solnet) als auch mit öffentlichen Proxies (zufällige Auswahl)[35] ➢ Internet-Zugriffsversuche mittels lokalem Web-Proxy[36], welcher ebenfalls im Browser als Proxy eingetragen werden muss und lokal auf dem Benutzer-PC ausgeführt wird ➢ Zugriffsversuche auf öffentlich frei zugänglichen Online-Web-Proxy[37] (keine Proxy-Einstellungen im Browser nötig)	Sobald im Browser (sowohl Internet Explorer als auch Mozilla) ein externer Proxy-Server konfiguriert wird, ist bei aktiviertem Web-Proxy-Filter kein Internetzugriff mit dem Browser mehr möglich. Anders sieht die Sache aus, wenn anstelle eines externen Proxy-Servers ein lokaler Web-Proxy im Browser eingerichtet wird. Eine Verbindung ins Internet ist über diesen Proxy trotz aktiviertem Filter möglich. Verständlicherweise funktioniert auch der direkte Zugriff auf den Online-Web-Proxy im Internet ohne Probleme, da ja keine Proxy-Einstellungen direkt im Browser vorgenommen wurden.	✓

Tabelle 14: SonicWALL SOHO3 Content-Filtering – durchgeführte Tests und Ergebnisse

[32] tomsplace, siehe http://www.tomsplace.ch
[33] Swiss-Homepage, siehe http://www.swiss.com/net/index/tg-ob-mp-create-and-change.htm
[34] Amazon-Homepage, siehe http://www.amazon.de
[35] Free Proxy Public Servers List, siehe http://tools.rosinstrument.com/proxy/
[36] JAP Anonymity & Privacy, siehe http://anon.inf.tu-dresden.de/
[37] Guardster-Homepage, siehe http://www.guardster.com/

Im Bereich des URL-Filtering hat der Firewall-Administrator die Möglichkeit, die Zugriffsversuche für Angebote in den folgenden Kategorien nur aufzuzeichnen (zu loggen) oder aufzuzeichnen und zu blockieren:

Kategorie	***Erläuterungen***
Violence/Profanity	Umfasst gewalttätige Bilder und Texte gegen Menschen und Tiere
Gross Depictions	Umfasst vulgäre und unsittliche Bilder und Texte
Militant/Extremist	Umfasst ungesetzliche militante und/oder extremistische Bilder und Texte und Anleitungen zum Bau von Waffen und zur Herstellung von Sprengstoff
Questionable/Illegal Gambling	Umfasst Bilder und Texte mit dubiosem Charakter, welche unter Umständen illegal sind (inkl. Computer-Hacking und Software-Piraterie)
Partial Nudity	Umfasst Bilder, auf welchen die weibliche Brust und/oder das weibliche oder männliche Gesäss abgebildet sind
Full Nudity	Umfasst Bilder, auf welchen Genitalien abgebildet sind
Sexual Acts	Umfasst Texte und Bilder, welche sexuelle Handlungen beschreiben oder aufzeigen (inkl. Reklame für Telefonsex und Dating-Dienste und CD-ROMs und Videos mit entsprechendem Material)
Sex Education	Umfasst Texte und Bilder, welche den korrekten Gebrauch von Empfängnisverhütungsmitteln aufzeigen
Intolerance	Umfasst rassistische und anderweitig diskriminierende Texte und Bilder
Satanic/Cult	Umfasst Texte und Bilder, welche den Teufel anbeten oder irgend einen Kult propagieren
Alcohol & Tobacco	Umfasst Texte und Bilder, welche den Alkohol und den Tabak bewerben oder deren Konsum befürworten
Drugs/Drug Culture	Umfasst Texte und Bilder, welche den illegalen Gebrauch von Drogen befürworten (ausgenommen der Drogen, die im medizinischen Umfeld Verwendung finden)

Tabelle 15: SonicWALL SOHO3 – Filter-Kategorien für das URL-Filtering

Damit das URL-Filtering aktiviert werden kann, muss sich der Firewall-Administrator zuerst bei SonicWALL registrieren lassen, danach kann eine Filterliste aus dem Internet heruntergeladen werden, welche die zu blockenden Angebote enthält. Dieser Dienst kann während eines Monats kostenlos getestet bzw. eingesetzt werden (inkl. regelmässigen Filter-Listen-Updates).

Beim Internet-Zugriff eines Benutzers wird bei aktiviertem URL-Filtering überprüft, ob sich das vom Benutzer angeforderte Web-Angebot in der Filterliste befindet. Wenn dies der Fall ist, erhält der Benutzer anstelle der Webseite einen Hinweis, welcher durch den Firewall-Administrator frei definiert werden kann. Wenn sich das angeforderte Angebot nicht in der Filterliste befindet, wird die Webseite ganz normal angezeigt.

Es lässt sich festlegen, wann (permanent, nur zu bestimmten Tageszeiten und/oder nur an bestimmten Wochentagen) die entsprechenden URL-Filter gelten sollen. Auf das Content-Filtering haben diese Zeiteinschränkungen jedoch keinen Einfluss.

Mittels der „Consent"-Option (Zustimmung, Einwilligung) kann das URL-Filtering auch nur für explizit aufgeführte Arbeitsstationen aktiviert werden (bis zu 128 IP-Adressen von zu blockenden Arbeitsstationen lassen sich erfassen). Die übrigen Arbeitsstationen erhalten eine Einwilligungs- bzw. Zustimmungserklärung (zu vergleichen mit einer Internet-Policy), welche sie vor dem Surfen akzeptieren müssen. Die Benutzer können dabei wählen, ob sie mit aktiviertem URL-Filtering surfen wollen oder nicht. An gleicher Stelle lassen sich auch zeitliche Limiten für das Surfen festlegen. Danach erscheint eine Meldung, dass das Zeitlimit aufgebraucht sei.

Um nun die Wirksamkeit der Filterfunktion zu testen, wurden diverse Tests durchgeführt, welche sich grundsätzlich auf alle Kategorien beziehen. Es wurde bewusst darauf verzichtet, jede Kategorie einzeln zu begutachten und zu bewerten. Die folgende Zusammenstellung gibt einen Überblick über die durchgeführten Versuche und den daraus resultierenden Ergebnissen:

Versuche / Aktivitäten	***Erkenntnisse / Ergebnisse***	
➢ Alle URL-Filter-Kategorien aktivieren ➢ Im Internet gezielt Seiten aus den Bereichen „Erotik, Pornographie" und „Computer-Hacking, Software-Piraterie" unter der Eingabe des jeweiligen **DNS-Namens** ansurfen	Die Mehrheit der stichprobenweise ausgesuchten Web-Seiten im Erotikbereich werden zuverlässig geblockt. Es fällt hingegen auf, dass keine einzige angesurfte Website aus dem Bereich „Computer-Hacking, Software-Piraterie" geblockt wird. Anscheinend wird durch den Filterhersteller dem Thema Erotik / Pornographie ein höherer Stellenwert zugemessen als dem Bereich Computer-Hacking / Software-Piraterie. Es gilt zu berücksichtigen, dass diese Erkenntnisse auf subjektiv vorgenommen Einzelstichproben und nicht auf einer repräsentativen umfangreichen Auswahl von Webseiten beruhen.	✓ ✘
➢ Im Internet gezielt Seiten aus dem Bereich „Erotik, Pornographie", welche im ersten Versuch erfolgreich geblockt wurden, unter der Eingabe ihrer **IP-Adresse** ansurfen	Auch wenn Anstelle des DNS-Namens die IP-Adresse der Ziel-Webseiten verwendet wird, werden die angesurften Webseiten mit der gleichen Zuverlässigkeit geblockt wie beim ersten Versuch.	✓
➢ Im Internet gezielt Seiten aus dem Bereich „Erotik, Pornographie", welche in den ersten beiden Versuchen erfolgreich geblockt wurden, unter der Eingabe ihrer **IP-Adresse als Dezimalzahl*** ansurfen	Auch wenn Anstelle des DNS-Namens oder der normalen IP-Adresse die IP-Adresse als Dezimalzahl verwendet wird, werden die angesurften Webseiten mit der gleichen Zuverlässigkeit geblockt wie bei den ersten beiden Versuchen.	✓
➢ Einrichten eines lokalen Web-Proxies[38], welcher im Browser	Unter Verwendung eines lokalen Web-Proxies kann ohne Probleme auf alle Webseiten zugegrif-	

[38] JAP Anonymity & Privacy, siehe http://anon.inf.tu-dresden.de/

Versuche / Aktivitäten	***Erkenntnisse / Ergebnisse***	
als Proxy-Server eingetragen wird; im Internet gezielt Seiten aus dem Bereich „Erotik, Pornographie“, welche in den ersten drei Versuchen erfolgreich geblockt wurden, ganz normal über ihren DNS-Namen ansurfen	fen werden. Die Firewall „sieht“ nur die Verbindung (IP-Adresse) zum Web-Proxy-Anbieter und hat keine Kenntnis von den letztlich angesurften Webseiten. Auf diese Weise kann sie den Zugriff auf die an und für sich nicht zugelassenen Webseiten auch nicht unterbinden.	
➢ Verbindung zu dem öffentlich frei zugänglichen Online-Web-Proxy „Guardster“[39] und zum „Web Page Backward Compatibility Viewer“[40] herstellen; über beide Dienste gezielt Seiten aus dem Bereich „Erotik, Pornographie“, welche in den ersten drei Versuchen erfolgreich geblockt wurden, ganz normal über ihren DNS-Namen ansurfen	Im Unterschied zur ZyXEL ZyWALL 10W kann mit der SonicWALL-Firewall zum getesteten Online-Web-Proxy „Guardster“ keine Verbindung aufgenommen werden, da die Website in der URL-Filter-Liste von SonicWALL registriert ist; der Zugriff wird somit durch die Firewall geblockt.	✓ ✘
➢ Webseiten aus dem Bereich „Erotik, Pornographie“, welche in den ersten drei Versuchen erfolgreich geblockt wurden, über die Suchmaschine „Google“[41] ausfindig machen und diese mittels Übersetzungsdienst von „Google“ übersetzen lassen	Beim Zugriff auf nicht zugelassene Webseiten mittels dem „Web Page Backward Compatibility Viewer“ und dem „Google“-Übersetzungsdienst werden die Webseiten nicht geblockt; dem Benutzer werden jedoch nur die Textpassagen der nicht zugelassenen Webseiten, aber nicht die Bilder, angezeigt.	

Tabelle 16: SonicWALL SOHO3 URL-Filtering – durchgeführte Tests und Ergebnisse

* Siehe dazu die Erklärungen, welche bei der Analyse der ZyWALL unter Kapitel 5.3.1 an entsprechender Stelle abgegeben wurden.

Die Filter-Liste der Firewall kann automatisch im wöchentlichen Intervall, immer zur gleichen Zeit, aktualisiert werden. Ausserdem lässt sich die heruntergeladene Filter-Liste durch weitere Einträge manuell ergänzen. Diese Einträge erfolgen über die Firewall-Administrationsoberfläche. Eine direkte Bearbeitung der heruntergeladenen Filter-Liste ist nicht möglich. Die manuelle Ergänzung der Filter-Liste kann sehr zeitaufwändig sein, da, identisch zur ZyXEL ZyWALL 10W, für einen effektiven Filter-Schutz neben dem Domänennamen der zu blockenden Internetseite auch ihre IP-Adresse sowohl in Normal- als auch Dezimalform eingetragen werden muss. Für einen umfassenden Zugriffsschutz sind somit pro Internetangebot ebenfalls drei manuelle Einträge nötig.

Zusätzlich besteht die Möglichkeit, vertrauenswürdige Domänen einerseits und erlaubte Domänen andererseits explizit zu definieren. Durch die Definition von vertrauenswürdigen Do-

[39] Guardster-Homepage, siehe http://www.guardster.com/
[40] Web Page Backward Compatibility Viewer, siehe http://www.delorie.com/web/wpbcv.html
[41] Google-Suchmachine, siehe http://www.google.com

männen können Java-Applets, ActiveX-Controls, Cookies und Web-Proxies (also die Elemente des Content-Filterings), welche von diesen Domänen stammen, zugelassen werden. Durch die Festlegung von erlaubten Domänen lassen sich einzelne Webseiten vom URL-Filtering ausschliessen, damit ein Zugriff auf diese möglich ist, obwohl sie eigentlich in der Filter-Liste eingetragen sind. Zudem kann der Zugriff auf das Internet auf die explizit erlaubten Domänen eingeschränkt werden.

Als letzte Variante des Zugriffsschutzes kann der Firewall-Administrator definieren, welche Zeichenfolgen nicht in der URL vorkommen dürfen (identisch zur ZyXEL ZyWALL 10W). So hat der Ausschluss der Zeichenfolge „hsw“ zur Folge, dass die Internetseite der Hochschule für Wirtschaft in Luzern über ihren Domänennamen „www.hsw.fhz.ch“ nicht mehr aufgerufen werden kann. Auch eine solche Sperre lässt sich natürlich problemlos umgehen, indem anstatt des Domänennamens die IP-Adresse eingegeben wird.

Fazit Content- und URL-Filtering

Obschon die Content- und URL-Filtering-Funktionen bei der SonicWALL SOHO3 in der Gesamtbetrachtung besser zu gefallen wissen als bei der ZyXEL ZyWALL 10W, verhält sich auch bei dieser Firewall das Cookie-Filtering nicht wie erwartet. Die manuellen Erweiterungen im Bereich des URL-Filtering erscheinen ebenfalls nur bedingt praxistauglich, da der Zeitaufwand zur Erfassung und Pflege dieser Erweiterungen nicht unterschätzt werden darf und deren Wirksamkeit zum Teil mit trivialsten Mitteln untergraben werden kann.

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen 😐

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Die Firewall verfügt über Content-Filter für ActiveX-Controls, Java-Applets, Cookies, Web-Proxies und bekannte gefälschte digitale Zertifikate
- Die Firewall unterstützt die Anbindung an URL-Filtering-Software von Drittherstellern
- Eine Vielzahl von URL-Filtering-Kategorien, welche einzeln aktiviert oder deaktiviert werden können, stehen zur Verfügung
- Die Einträge der URL-Filter-Liste können durch manuelle Einträge direkt auf der Firewall ergänzt werden
- Das URL-Filtering funktioniert bei den in der Filter-Liste vorhandenen Einträgen sowohl basierend auf dem DNS-Namen als auch basierend auf der IP-Adresse und der dezimalisierten IP-Adresse zuverlässig
- Eine Internet-Policy, welche der Benutzer akzeptieren muss, kann vor dem Zugriff auf das Internet eingeblendet werden
- In der URL-Filter-Liste sind anscheinend auch Online-Web-Proxy-Dienste eingetragen; auf diese Weise kann dem Umgehen der URL-Filter Einhalt geboten werden

⊖

- Der Content-Filter für Cookies scheint ziemlich wirkungslos zu sein oder verhält sich auf jeden Fall nicht wie erwartet
- Die URL-Filter-Liste scheint nicht alle Filter-Kategorien gleich umfassend abzudecken; ein Schwergewicht besteht anscheinend auf dem Bereich „Erotik, Pornographie“
- Das Pflegen von manuellen URL-Filter-Einträgen ist sehr zeitaufwendig, da die Einträge für ein wirksames URL-Filtering immer in Form des DNS-Namens, der IP-Adresse und der dezimalisierten IP-Adresse eingegeben werden müssen
- Alle Content- und URL-Filter können mit einem lokalen Web-Proxy umgangen werden; der Einsatz eines lokalen Web-Proxies kann durch die Firewall nicht verhindert werden

6.3.4 Virenprüfung

SonicWALL bietet in ihrer Firewall in Zusammenarbeit mit dem Anti-Virensoftwarehersteller McAfee die Anti-Virenlösung „VirusScan ASaP“ an. Diese Dienstleistung kann während eines Monats in einer 5-Benutzer-Lizenz kostenlos getestet werden.

Die Firewall prüft, sobald ein LAN-Benutzer auf das Internet zugreifen will, ob auf seinem System die Anti-Virensoftware „VirusScan ASaP“ installiert ist. Falls dies nicht der Falls sein sollte, wird der Internetzugriff verwehrt und der Benutzer wird aufgefordert die Anti-Virensoftware zu installieren (siehe Abbildung 16).

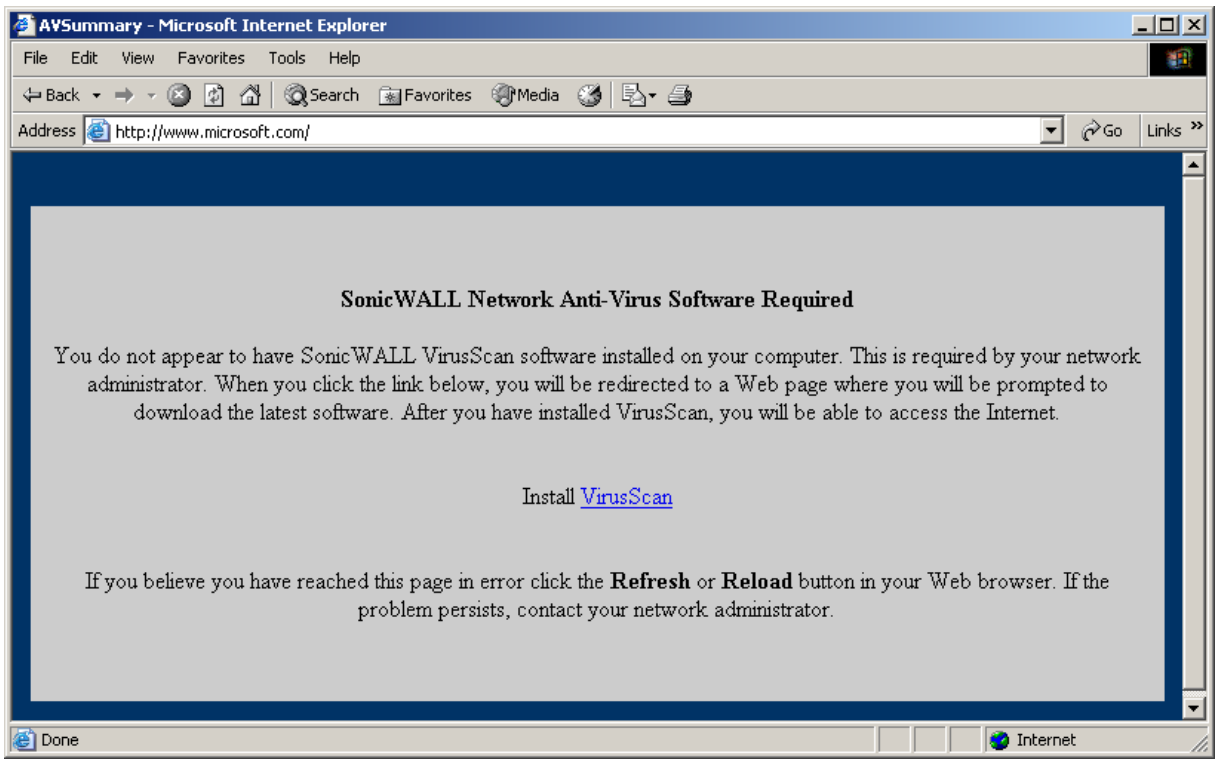

AVSummary - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.microsoft.com/
Go Links
SonicWALL Network Anti-Virus Software Required
You do not appear to have SonicWALL VirusScan software installed on your computer. This is required by your network administrator. When you click the link below, you will be redirected to a Web page where you will be prompted to download the latest software. After you have installed VirusScan, you will be able to access the Internet.
Install VirusScan
If you believe you have reached this page in error click the Refresh or Reload button in your Web browser. If the problem persists, contact your network administrator.
Done
Internet

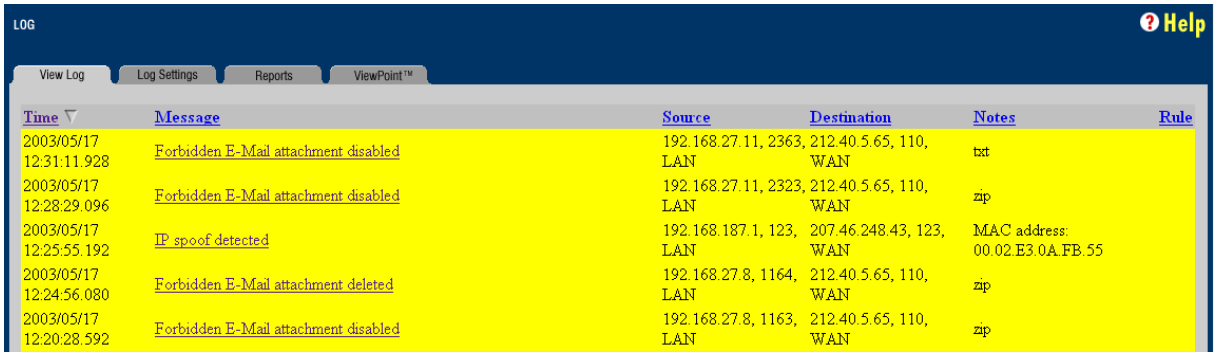
Abbildung 16: SonicWALL SOHO3 – Aufforderung zur Installation des Anti-Virenprogramms

Auf der Firewall kann definiert werden, welche Clients über diese Anti-Virensoftware verfügen müssen, wenn sie auf das Internet zugreifen wollen. Entweder unterliegen alle Systeme dieser Anti-Virenpolicy oder aber es können IP-Adressbereiche explizit einbezogen oder aber davon ausgeschlossen werden.

Nach Aktivierung des Anti-Virendienstes sendet die Firma SonicWALL an SonicWALL-Firewalls, welche über diesen Dienst verfügen, Warnmeldungen zu aktuellen Viren. Diese Warnmeldungen werden an die in der Firewall definierte „Alert“-E-Mail-Adresse gesendet und im Firewall-Log festgehalten. Ausserdem müssen die Benutzer nach der Warnmeldung zwingend ein Update der Anti-Virensoftware durchführen, bevor sie wieder auf das Internet zugreifen dürfen.

Der Anti-Virendienst verfügt auch über einen E-Mail-Filter, bei welchem definiert werden kann, welche Attachments (aufgrund ihrer Dateinamenserweiterung) aus E-Mails herausgefiltert werden sollen. Dabei kann der Administrator festlegen, ob die Dateinamenserweiterung des Attachments einfach umbenannt und das Attachment dem Endbenutzer trotzdem zuge-

stellt oder aber ob das Attachment direkt durch die Firewall gelöscht werden soll. So oder so erhält der Endbenutzer zum gefilterten E-Mail noch eine Textnachricht mit einer entsprechenden Warnmeldung. Welche E-Mails mit welchen Attachments von der Firewall gefiltert wurden, wird auch in der Firewall-Logdatei vermerkt (siehe Abbildung 17).



Time	Message	Source	Destination	Notes	Rule
2003/05/17 12:31:11.928	Forbidden E-Mail attachment disabled	192.168.27.11, 2363, LAN	212.40.5.65, 110, WAN	txt	
2003/05/17 12:28:29.096	Forbidden E-Mail attachment disabled	192.168.27.11, 2323, LAN	212.40.5.65, 110, WAN	zip	
2003/05/17 12:25:55.192	IP spoof detected	192.168.187.1, 123, LAN	207.46.248.43, 123, WAN	MAC address: 00.02.E3.0A.FB.55	
2003/05/17 12:24:56.080	Forbidden E-Mail attachment deleted	192.168.27.8, 1164, LAN	212.40.5.65, 110, WAN	zip	
2003/05/17 12:20:28.592	Forbidden E-Mail attachment disabled	192.168.27.8, 1163, LAN	212.40.5.65, 110, WAN	zip	

Abbildung 17: SonicWALL SOHO3 – Log-Einträge gefilterter Attachments

Als weitere Option steht noch zur Verfügung, dass E-Mail-Fragmente durch die Firewall geblockt werden sollen, um damit die Einschleusung von Viren, welche über mehrere E-Mail-Fragmente verteilt zugestellt werden, zu verhindern.

Fazit Virenprüfung

Obschon die angebotene Anti-Virendiensleistung sicher auch ihre Vorteile hat, stellt sich die Frage, ob das Anti-Viren-Management auf einem anderen (dedizierten) System nicht besser aufgehoben wäre. Ein umfassendes Anti-Virenschutzkonzept muss sicherstellen, dass auch Systeme, welche nicht auf das Internet zugreifen, über einen aktuellen Virenschutz verfügen. Eine Verteilung der aktuellen Anti-Virensignaturen über Login-Scripts oder ähnliche Mechanismen kann diese Anforderung besser erfüllen, als ein System, bei welchem der Virenschutz „erst“ beim Zugriff auf das Internet auf sein Vorhandensein und die Aktualität überprüft wird. Trotz dieser „Kritikpunkte“ funktionierte die in der SonicWALL implementierte Anti-Virenfunktion problemlos.

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Die Firewall kann sicherstellen, dass alle Windows-Clients, welche auf das Internet zugreifen wollen, über eine aktuelle Anti-Virensoftware verfügen
- E-Mail-Attachments lassen sich aufgrund ihrer Dateinamenserweiterung durch die Firewall filtern
- Die Firma SonicWALL kann die Firewall-Administratoren auf neue Virengefahren automatisch aufmerksam machen und die Firewall lässt in einem solchen Fall den Zugriff auf das Internet erst wieder nach der Installation der aktuellsten Version der Anti-Virensoftware zu

⊖

- Systeme, welche selber nicht auf das Internet zugreifen, verfügen unter Umständen über keinen oder keinen aktuellen Virenschutz

- Auch wenn ein umfassender Virenschutz auf eine andere Weise vielleicht besser realisiert werden kann, trägt die implementierte Anti-Virenfunktion zur Erhöhung der Sicherheit der internen Systeme bei

6.3.5 „Intrusion Detection"-Funktionen, Anti-Spoofing

Auf der Firewall ist standardmässig eine „Intrusion Detection"-Funktion aktiviert. Zu dieser Funktion können keine individuellen Einstellungen vorgenommen werden und sie lässt sich auch nicht deaktivieren. Auf diese Weise sollen allfällige DoS- (Denial of Service) und andere Attacken möglichst frühzeitig erkennt und geloggt werden. Gemäss Firewall-Onlinehilfe erkennt die Firewall folgende Attacken:

- DoS-Attacken
  - Ping of Death
  - SYN flooding
  - Land
  - Smurf
- Trojaner-Viren
  - Back Orifice (TCP-Port 31337)
  - IniKiller (TCP-Port 9989)
  - NetBus (keine Hinweise in der Online-Hilfe auf die geblockten TCP-Ports)
  - NetSpy (TCP-Port 1024)
  - Priority (TCP-Port 16969)
  - Ripper (TCP-Port 2023)
  - Senna Spy (TCP-Port 13000)
  - Striker (TCP-Port 2565)
  - SubSeven (TCP-Ports 6667, 6711, 27374)
- IP Spoofing auf LAN- und WAN-Interface
- Portscans
- Stealth Scanning (spezielle Arten von Portscans wie TCP FIN, Stealth FIN, Xmas Tree, Null Scan)
- E-Mail Fragmente
- FTP PASV Response Spoof

Das IP-Spoofing auf dem externen und internen Interface der Firewall und alle durchgeführten Portscan-Attacken[42] aus dem WAN auf das externe Interface der Firewall wurden korrekt durch die Firewall registriert und aufgezeichnet. Die Firewall hat sogar die verschiedenen Portscan-Varianten wie FIN-, NULL-, XMAS-Scan usw. einwandfrei erkannt (siehe Abbildung 18).

[42] Die Portscans wurden mit dem Programm „nmap" durchgeführt (www.insecure.org)

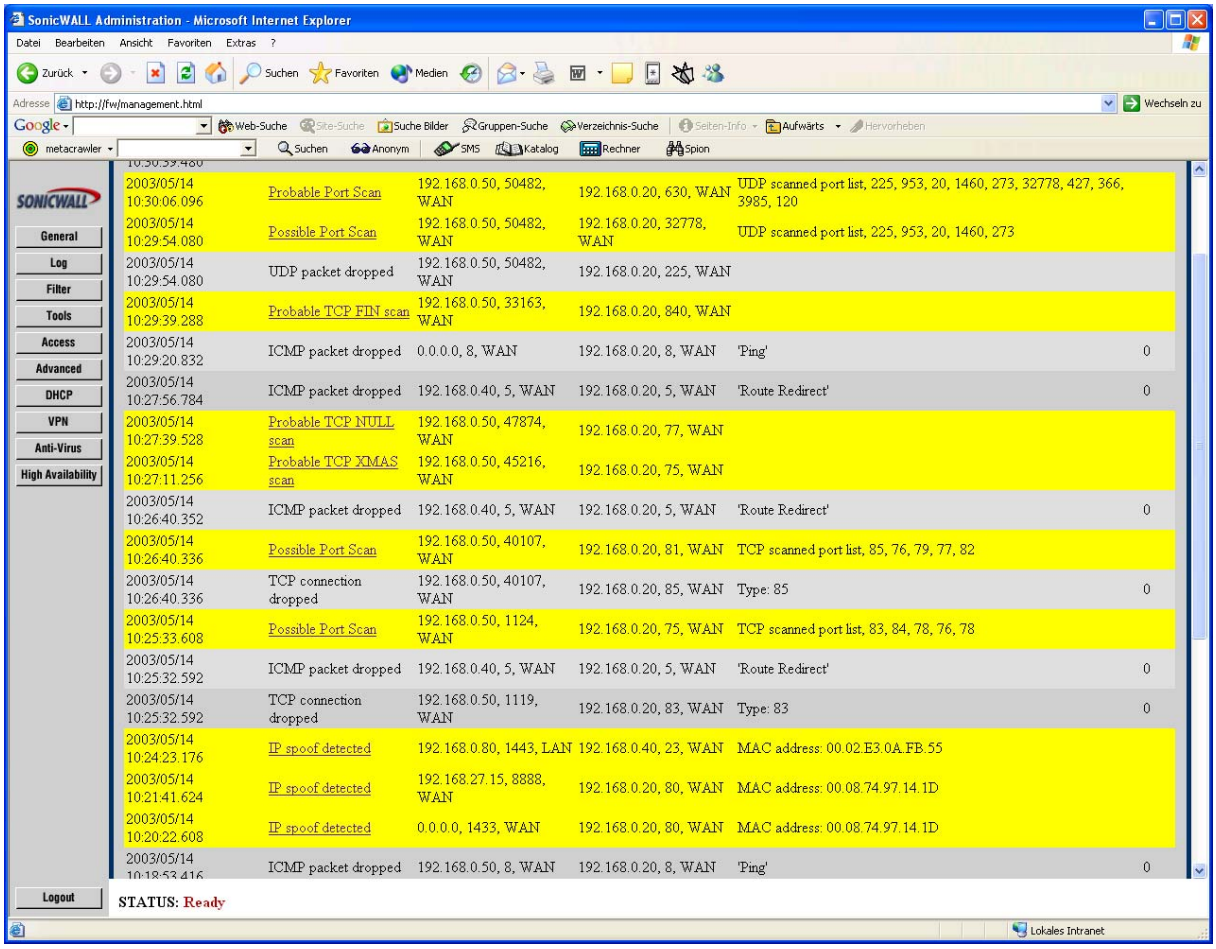


Abbildung 18: SonicWALL SOHO3 – Durch die Firewall korrekt erkannte Attacken

Portscans aus dem LAN auf das interne Interface der Firewall werden durch diese jedoch nicht festgestellt. Die „Intrusion Detection"-Funktion der Firewall konzentriert sich offensichtlich primär auf das externe Interface der Firewall und somit auf Angriffe aus dem WAN bzw. Internet.

Trojaner-Zugriffsversuche werden durch die Firewall ebenfalls erkannt. Tests mit dem Trojaner-Virus „SubSeven" haben ergeben, dass die Firewall diesen erkennt, solange der Standard-Port (TCP-Port 27374) des Trojaners verwendet wird. Wenn der Trojaner über einen anderen Port auf das System zugreifen will (im durchgeführten Versuch z.B. auf TCP-Port 8889), blockt die Firewall zwar diesen Port, erkennt den Trojaner jedoch nicht mehr als solchen (siehe Abbildung 19).

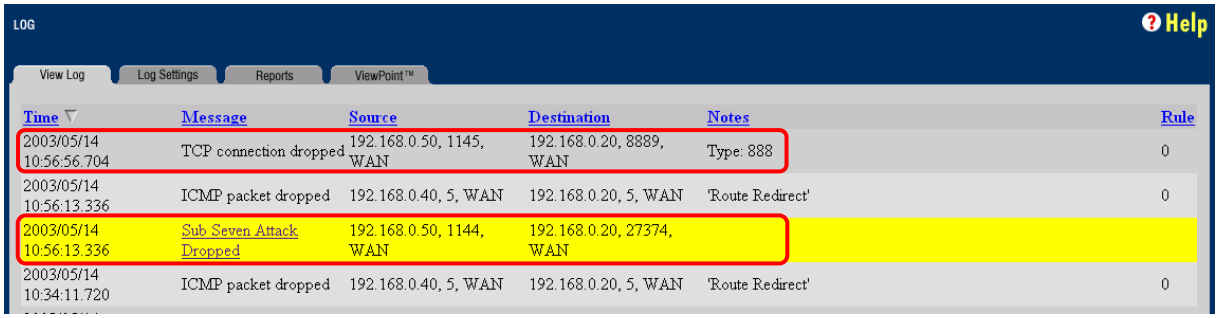


Abbildung 19: SonicWALL SOHO3 – Erkennung von Trojaner-Zugriffsversuchen

Fazit „Intrusion Detection"-Funktion, Anti-Spoofing

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Die Firewall erkennt allfällige DoS- oder andere Attacken zuverlässig und alarmiert den Firewall-Administrator unmittelbar per E-Mail
- Portscans auf das externe Interface der Firewall werden als solche unabhängig vom gewählten Verfahren erkannt
- IP-Spoofing wird sowohl auf dem internen als auch auf dem externen Interface der Firewall erkannt

⊖

- Portscans auf das interne Interface der Firewall werden durch die Firewall nicht als Attacke erkannt

6.3.6 Logging-Möglichkeiten, Alarmierung und Überwachung der Internetaktivitäten

Die Log-Einträge werden in verschiedene Kategorien unterteilt. Die Einträge in der Log-Datei können jedoch nicht direkt auf der Firewall nach Kategorie gefiltert und gesondert ausgegeben werden. Nachfolgende Tabelle gibt einen Überblick über die vorhandenen Kategorien und ob bei einem neuen Log-Eintrag in eine der Kategorien ein unmittelbarer Alarm an eine E-Mail-Adresse ausgelöst werden kann oder nicht:

Bezeichnung des Logs	***Erläuterungen zum Inhalt***	***Unmittelbare Alarmierung möglich***
System Maintenance	Administrator-Logins, automatisches Laden der Filter-Liste, aktivieren und zurücksetzen der Firewall usw.	nein
System Errors	Probleme mit DNS, E-Mail und dem automatischen Laden der Filter-Liste	ja
Blocked Web Sites	Webseiten, Newsgroups oder andere Dienste, welche durch die Filter-Liste oder durch ein Stichwort geblockt wurden	ja

Bezeichnung des Logs	***Erläuterungen zum Inhalt***	***Unmittelbare Alarmierung möglich***
Blocked Java etc.	Java-Applets, ActiveX-Controls und Cookies, welche durch die SonicWALL entfernt bzw. geblockt wurden	nein
Attacks	SYN-Flooding, Ping of Death, IP Spoofing und Versuche, die Firewall aus dem Internet über das externe Interface zu administrieren	ja
VPN TCP Status	VPN-Verkehrsinformationen inkl. Datentransfers durch VPN-Tunnels	ja
User Activity	Erfolgreiche und abgewiesene Benutzer-Logins	nein
Dropped TCP	Eingehende zurückgewiesene TCP-Verbindungen	nein
Dropped UDP	Eingehende zurückgewiesene UDP-Verbindungen	nein
Dropped ICMP	Eingehende zurückgewiesene ICMP-Verbindungen	nein
Network Debug	Ethernet-Broadcasts, ARP Auflösungsprobleme, ICMP Umleitungsprobleme und NAT-Probleme. Auf diese Weise sollen Probleme in der Netzwerkkonfiguration analysiert werden können	nein
Denied LAN IP	Untersagte TCP- oder UDP-Pakete aus dem internen Netzwerk	nein

Tabelle 17: SonicWALL SOHO3 – Logging-Kategorien

Jede Kategorie kann für das Logging und, dort wo vorhanden, auch für die Alarmierung einzeln aktiviert oder deaktiviert werden. Der Informationsgehalt der einzelnen Log-Einträge (Datum, Uhrzeit, kurze Meldung, Quell-Adresse und Quell-Port, Ziel-Adresse und Ziel-Port, betroffene Regel) entspricht den minimalen Anforderungen. Es besteht die Möglichkeit, die Log-Einträge, sobald die Log-Datei voll ist oder in einem anderen zu definierenden Intervall, automatisch an eine E-Mail-Adresse zu versenden oder noch besser direkt an einen Syslog-Server weiterzuleiten.

Die Firewall verfügt auch über eine Reporting-Funktion. Der Firewall-Administrator kann per Mausklick eine so genannte Datensammlung initiieren und diese nach einer beliebigen Zeit wieder stoppen. Danach kann für alle während der Aufzeichnungszeit erfolgten Zugriffe vom internen ins externe Netzwerk bzw. Internet eine Rangreihenfolge bezüglich folgender Kriterien erstellt werden:

- Anzahl Website-Hits einer besuchten Internet-Adresse
- Benutzte Bandbreite pro IP-Adresse
- Benutzte Bandbreite pro Dienst

Für weiterführende Auswertungen kann zudem die in der Firewall implementierte Funktion „ViewPoint“ eingesetzt werden. Diese muss jedoch als „Upgrade“ zur Firewall käuflich erworben werden.

Fazit Logging-Möglichkeiten, Alarmierung und Überwachung Internetaktivitäten

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen 😐

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Verschiedene Log-Kategorien stehen zur Verfügung, welche einzeln aktiviert oder deaktiviert werden können
- Unmittelbare Alarmierung einzelner Ereignisse möglich
- Die Log-Einträge können automatisch an eine E-Mail-Adresse und/oder einen Syslog-Server gesendet werden
- Der Internet-Verkehr lässt sich überwachen und basierend darauf können Analysen bezüglich benötigter Bandbreiten vorgenommen werden

⊖

- In den Log-Einträgen kann nicht gesucht werden (nur über die normale Suchfunktion des Internet-Browsers)
- Die Log-Einträge lassen sich nicht filtern

6.3.7 Network Address Translation (NAT)

Die SonicWALL SOHO3 unterstützt sowohl dynamisches als auch statisches NAT, wobei beim statischen NAT zwei Varianten zur Auswahl stehen. Folgende Tabelle gibt einen Überblick über die NAT-Konfigurationsmöglichkeiten:

NAT-Bezeichnung SonicWALL	Typ	Interne IP-Adresse(n)	Externe IP-Adresse(n)
NAT Enabled / NAT with DHCP Client	dynamisch	192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 […]	80.254.159.30
One-to-One NAT	statisch	192.168.1.10 192.168.1.11 192.168.1.12	80.254.159.30 80.254.159.31 80.254.159.32
Public LAN Server	statisch	192.168.1.10 (Port 80) 192.168.1.20 (Port 25)	80.254.159.30 (Port 80) 80.254.159.30 (Port 25)

Tabelle 18: SonicWALL SOHO3 – NAT-Konfigurationsmöglichkeiten

Von gewissem Interesse ist sicher die NAT-Variante „Public LAN Server“ (entspricht der Variante „Server“ bei der ZyXEL ZyWALL 10W Firewall), da auf diese Weise einer öffentlichen IP-Adresse je nach Dienst (Port) ein unterschiedliches internes Zielsystem (mit privater IP-

Adresse) zugeordnet werden kann. Die Vor- und Nachteile einer solchen Konfiguration wurden bereits im Kapitel 5.3.4 (ZyXEL ZyWALL 10W) beschrieben.

Fazit NAT

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs -

⊕

- Die Firewall unterstützt sowohl dynamisches als auch statisches NAT
- Durch NAT sind die internen Systeme aus dem Internet nicht direkt ersichtlich

⊖

- Allfällig angebotene Server-Dienste im internen Netzwerk stellen ein gewisses Risiko dar

6.3.8 DHCP-Server

Der DHCP-Server lässt sich aktivieren und deaktivieren. Folgende Einstellungen sind möglich:

- Startadresse des Bereichs der zu vergebenden IP-Adressen
- Grösse des Bereichs der zu vergebenden IP-Adressen
- LAN-Default-Gateway (bei Einsatz von NAT ist das Default-Gateway die Firewall selber, sonst ein anderer Router im Netzwerk)
- IP-Adressen von drei DNS-Servern
- IP-Adressen von zwei WINS-Servern

Ausserdem können für einzelne Clients auch statische IP-Adressen vergeben werden (so genanntes statisches DHCP). Dabei erfolgt die Zuteilung der immer gleichen IP-Adresse aufgrund der Hardwareadresse (MAC-Adresse) der Netzwerkkarte des Clients.

Fazit DHCP-Server

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs -

⊕

- Alle wesentlichen DHCP-Einstellungen können vorgenommen werden
- Es wird sowohl dynamisches als auch statisches DHCP unterstützt

⊖

6.3.9 Zeitserver-Dienst

Die SonicWALL SOHO3 kann ihre Systemzeit ebenfalls von einem Zeitserver beziehen. Dabei kommt das NTP-Protokoll zum Einsatz. Standardmässig verfügt die Firewall über eine

interne Liste von Internet-Zeitservern. Aufzeichnungen des Netzwerkverkehrs nach Aktivierung der Zeitserver-Funktion haben gezeigt, dass die Firewall versucht, auf Zeitserver der Universität Erlangen in Deutschland (IP-Adressen 131.188.34.75 und 131.188.34.45), von welchen sie jedoch zum Zeitpunkt der Analyse keine Antwort erhalten hat, und auf einen Zeitserver in Frankreich (IP-Adresse 138.96.64.10) zuzugreifen. Vom Zeitserver in Frankreich konnte die Firewall letztlich die aktuelle Uhrzeit beziehen:

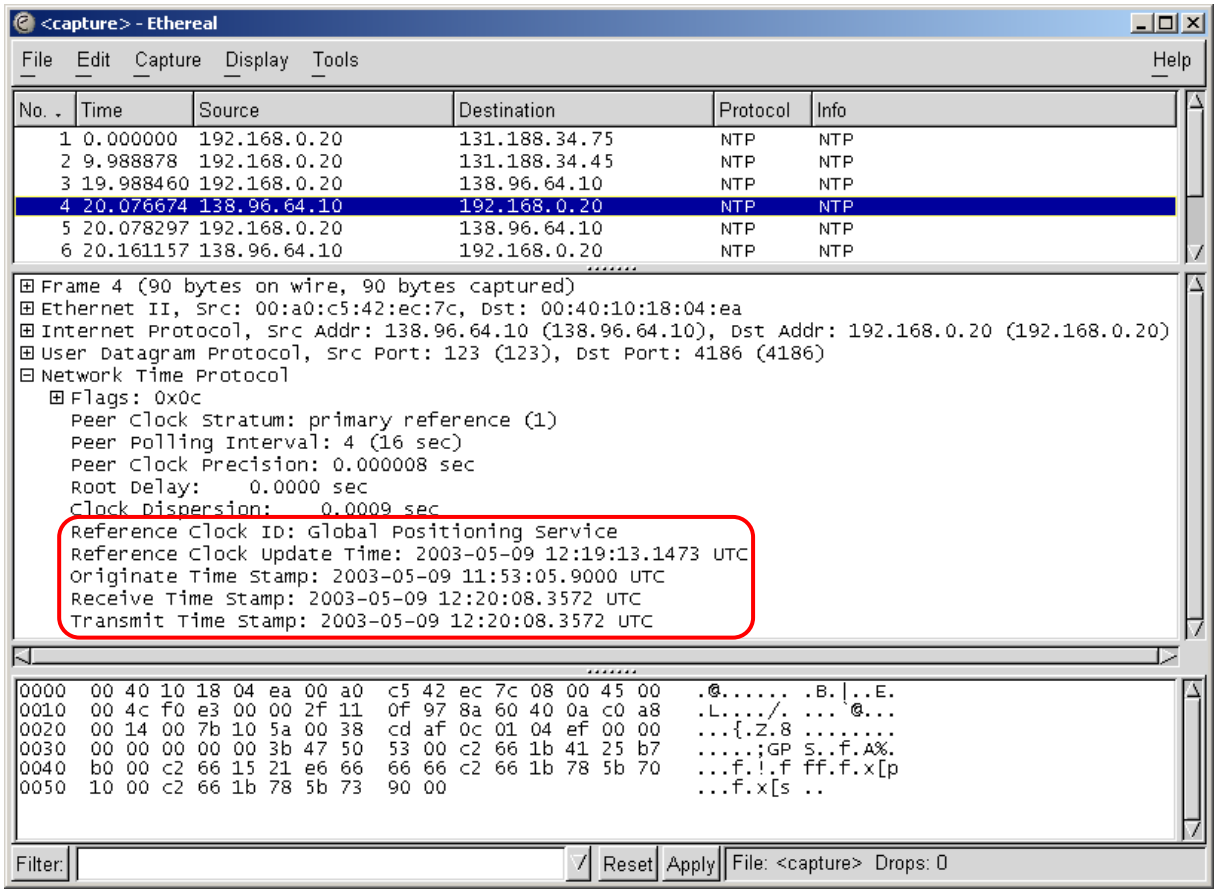

<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 0.000000 192.168.0.20 131.188.34.75 NTP NTP
2 9.988878 192.168.0.20 131.188.34.45 NTP NTP
3 19.988460 192.168.0.20 138.96.64.10 NTP NTP
4 20.076674 138.96.64.10 192.168.0.20 NTP NTP
5 20.078297 192.168.0.20 138.96.64.10 NTP NTP
6 20.161157 138.96.64.10 192.168.0.20 NTP NTP
Frame 4 (90 bytes on wire, 90 bytes captured)
Ethernet II, Src: 00:a0:c5:42:ec:7c, Dst: 00:40:10:18:04:ea
Internet Protocol, Src Addr: 138.96.64.10 (138.96.64.10), Dst Addr: 192.168.0.20 (192.168.0.20)
User Datagram Protocol, Src Port: 123 (123), Dst Port: 4186 (4186)
Network Time Protocol
Flags: 0x0c
Peer Clock Stratum: primary reference (1)
Peer Polling Interval: 4 (16 sec)
Peer Clock Precision: 0.000008 sec
Root Delay: 0.0000 sec
Clock Dispersion: 0.0009 sec
Reference Clock ID: Global Positioning Service
Reference Clock Update Time: 2003-05-09 12:19:13.1473 UTC
Originate Time Stamp: 2003-05-09 11:53:05.9000 UTC
Receive Time Stamp: 2003-05-09 12:20:08.3572 UTC
Transmit Time Stamp: 2003-05-09 12:20:08.3572 UTC
0000 00 40 10 18 04 ea 00 a0 c5 42 ec 7c 08 00 45 00 .@..... .B.|..E.
0010 00 4c f0 e3 00 00 2f 11 0f 97 8a 60 40 0a c0 a8 .L..../. ...`@...
0020 00 14 00 7b 10 5a 00 38 cd af 0c 01 04 ef 00 00 ...{.Z.8 ....
0030 00 00 00 00 00 3b 47 50 53 00 c2 66 1b 41 25 b7 .....;GP S..f.A%.
0040 b0 00 c2 66 15 21 e6 66 66 66 c2 66 1b 78 5b 70 ...f.!.f fff.f.x[p
0050 10 00 c2 66 1b 78 5b 73 90 00 ...f.x[s ..
Filter: Reset Apply File: <capture> Drops: 0

Abbildung 20: SonicWALL SOHO3 – Zeitabgleich mit Zeitserver

Der Firewall-Administrator hat jedoch auch die Möglichkeit, die IP-Adressen der zu konsultierenden Zeitserver manuell in der Firewall zu hinterlegen. So ist es möglich, netzwerkinterne Zeitserver als Referenz zu verwenden. Die Einstellung der eigenen Zeitzone und die Definition zum automatischen Umstellen der Systemzeit beim Wechsel von Sommer- auf Winterzeit und umgekehrt können ebenfalls vorgenommen werden. Das Update-Intervall beträgt standardmässig 60 Minuten, kann jedoch beliebig angepasst werden.

Fazit Zeitserver

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕ ⊖

- Firewall kann Systemzeit sowohl von Zeitservern aus dem Internet als auch von Zeitservern aus dem internen Netzwerk beziehen
- Update-Zeitintervall kann frei definiert werden
- Firewall und die wesentlichen internen Serversysteme erhalten alle ihre Systemzeit von einem zentralisierten Zeitserver, was die Nachvollziehbarkeit bei Zwischenfällen erhöht (erhöhte Sicherheit)

6.3.10 Virtual Private Network (VPN)

In der SonicWALL SOHO3 ist ebenfalls VPN basierend auf IPSec (Internet Protocol Security) integriert. Auch bei dieser Firewall werden, identisch zur ZyWALL 10W (siehe Kapitel 5.3.9), sowohl das ESP-Protokoll mit den kryptographischen Algorithmen DES und 3DES für die Vertraulichkeit und HMAC-MD5 und HMAC-SHA-1 für die Authentizität der Daten als auch das AH-Protokoll mit den kryptographischen Algorithmen HMAC-MD5 und HMAC-SHA-1 für die Authentizität der Daten unterstützt (siehe Abbildung 21).

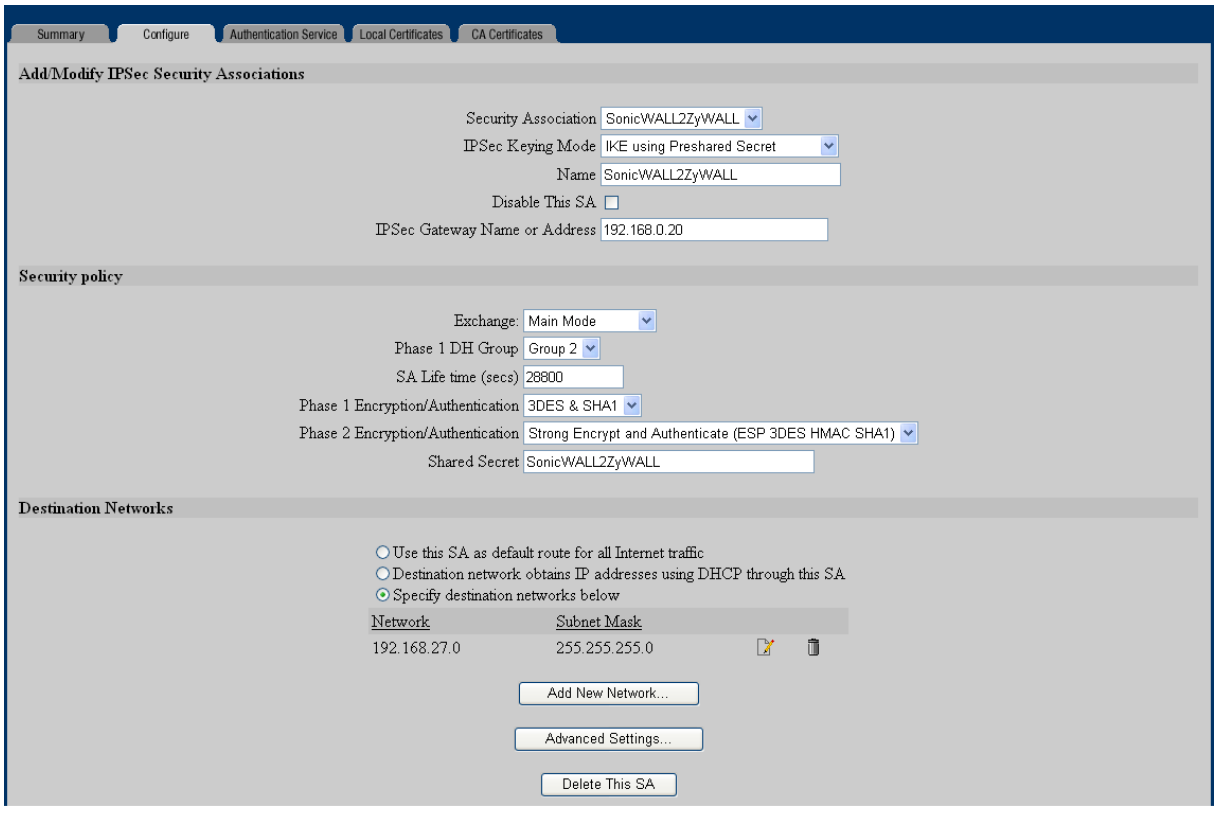


Abbildung 21: SonicWALL SOHO3 – VPN-Grundeinstellungen

Das Schlüsselmanagement kann manuell oder basierend auf dem IKE-Protokoll (Internet Key Exchange) erfolgen. Beim IKE-Protokoll können für die beiden Phasen der Schlüssel-

aushandlung individuelle Einstellungen betreffend der zu verwendenden Algorithmen und der Schlüsselstärke vorgenommen werden.

Die Tests bezüglich VPN-Interoperabilität zwischen der SonicWALL SOHO3 und der ZyWALL 10W (siehe auch Kapitel 5.3.9) und zwischen der SonicWALL SOHO3 und der Check Point Firewall-1 NG (siehe auch Kapitel 7.3.7) verliefen erfolgreich. Sowohl der VPN-Verbindungsaufbau zwischen der SonicWALL SOHO3 und der ZyWALL 10W als auch zwischen der SonicWALL SOHO3 und der Check Point Firewall-1 NG klappte, sogar mit den höchsten Sicherheitseinstellungen, ohne Probleme. Die dabei verwendeten VPN-Einstellungen und die zugrunde liegenden Konfigurationen der verschiedenen Firewalls sind im Anhang, in den Kapiteln 13.2.2, 13.2.3 und 13.2.4 ersichtlich.

Um die Tests zwischen der SonicWALL SOHO3 und der ZyWALL 10W durchzuführen, wurde folgende Versuchsumgebung aufgebaut:

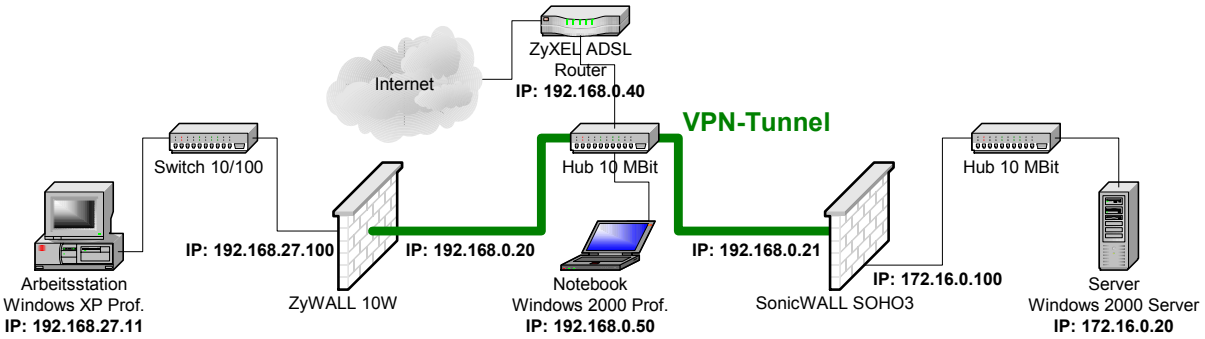


Abbildung 22: SonicWALL SOHO3 – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der ZyWALL 10W

Die VPN-Tests zwischen der SonicWALL SOHO3 und der Check Point Firewall-1 NG basierten auf folgender Versuchsumgebung:

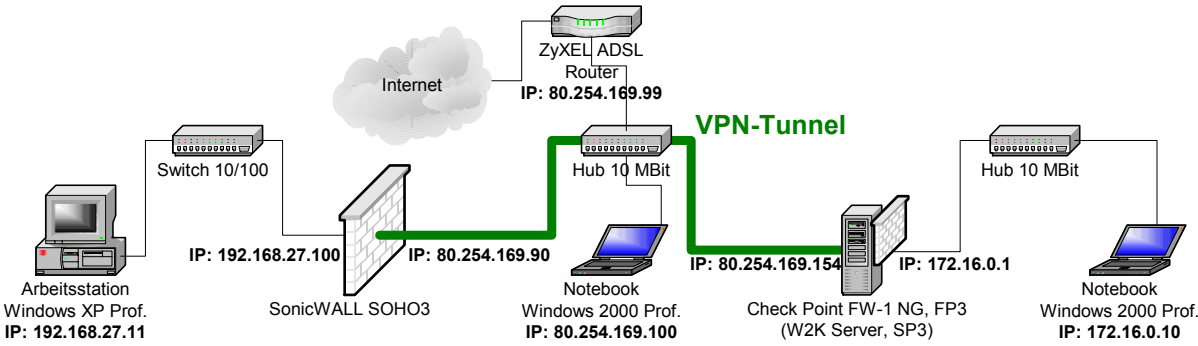


Abbildung 23: SonicWALL SOHO3 – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der Check Point Firewall-1 NG

Auch bei der SonicWALL wurde versucht, mittels Windows 2000 IPSec VPN-Client eine VPN-Verbindung zwischen einem Windows 2000 Notebook und der Firewall herzustellen. Diese Verbindung klappte, diesmal sogar mit den höchsten VPN-Sicherheitseinstellungen,

problemlos. Auch sonst traten mit der VPN-Implementation auf der SonicWALL-Firewall, im Unterschied zur ZyWALL, keine Instabilitäten oder anderweitige Probleme auf. Die Anleitung zur Konfiguration des IPSec-basierten VPN-Clients unter Windows 2000 ist im Anhang unter Kapitel 13.2.5 zu finden.

Fazit VPN

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕ ⊖

- Sichere (verschlüsselte) Netzwerkverbindungen mit anderen VPN-Gateways (z.B. anderen Firewalls) und zwischen VPN-Clients und Firewall möglich
- Interoperabilität mit anderen Firewalls
- Als VPN-Client kann Windows 2000 (oder höher) mit IPSec verwendet werden; keine Anschaffung eines dedizierten VPN-Clients nötig

6.3.11 Diagnosemöglichkeiten

Im Rahmen Diagnosemöglichkeiten stehen über das Web-GUI einige wenige Werkzeuge zur Verfügung. So können unter anderem ein DNS-Lookup, ein Ping und ein Traceroute durchgeführt oder ein „Tech Support Report“ erstellt werden. Dieser Report enthält alle wesentlichen Informationen zur aktuellen Konfiguration und zum Status der Firewall. Der Report gilt auch als Grundlage, wenn beim Firewall-Hersteller direkt um Hilfe nachgesucht wird.

Fazit Diagnosemöglichkeiten

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs -

⊕ ⊖

- Es stehen einige Diagnose-Werkzeuge zur Verfügung
- Ein umfangreicher Report, welcher alle wesentlichen Informationen zur Konfiguration und zum Status der Firewall beinhaltet, kann erstellt werden

6.3.12 Remote-Management

Das Remote-Management kann bei der SonicWALL SOHO3 mittels WWW (HTTP und HTTPS), VPN-Client (für das Firewall-Management aus dem Internet) und SNMP erfolgen. Standardmässig sind jedoch nur die Protokolle HTTP und HTTPS auf der Firewall aktiviert. Der Management-Zugriff ist grundsätzlich sowohl über das interne als auch das externe In-

terface der Firewall aus möglich. Um über das externe Interface zugreifen zu können, müssen jedoch zuerst entsprechende Firewall-Regeln definiert werden. Jedes der Managementprotokolle kann deaktiviert werden.

Analysen mit einem Sniffer haben bezüglich der Administrator-Passwortübermittlung im Netzwerk folgendes Ergebnis geliefert: Beim Management-Zugriff über das HTTP-Protokoll wird das Passwort nicht in Klartext, sondern als MD5-Hashwert transferiert. Beim Zugriff über HTTPS wird sowieso der ganze Netzwerkverkehr mittels SSL verschlüsselt.

Durch die „SonicWALL Global Management System (SGMS)"-Option kann die Firewall auch in einen Verbund von SonicWALL-Firewalls eingebunden werden, um damit ein einheitliches zentrales Management zu ermöglichen. Eine solche Anbindung kann ebenfalls durch VPN gesichert werden.

Fazit Remote-Management

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Mehrere Protokolle stehen für das Remote-Management zur Verfügung
- Das Remote-Management kann auch zentral für einen ganzen Verbund von SonicWALL-Firewalls über einen gesicherten VPN-Kanal erfolgen
- Das Firewall-Administrator-Passwort wird beim Zugriff über das HTTP-Protokoll nicht in Klartext, sondern als MD5-Hashwert über das Netzwerk transferiert
- Die Konfiguration mittels Web-GUI kann auch gesichert über das HTTPS-Protokoll erfolgen (SSL-Verschlüsselung des gesamten Netzwerkverkehrs)
- Jedes Remote-Management-Protokoll lässt sich einzeln aktivieren und deaktivieren

⊖

6.3.13 Firmware-Updates

Die Updates der Firewall-Firmware erfolgen manuell. Die jeweils aktuelle Firmware kann beim Hersteller heruntergeladen werden. Der Web-Konfigurator der Firewall verfügt über einen Menupunkt „Upload Firmware Now", über welchen die neue Firmware eingespielt werden kann. SonicWALL bietet zudem die Möglichkeit, sich automatisch informieren zu lassen, wenn eine neue Firmware verfügbar ist. Wenn diese Option aktiviert wird, werden einmal pro Tag Informationen über die eingesetzte Firewall (inkl. Firmwareinformationen) an die Firma SonicWALL gesendet. Falls eine neue Firmware vorliegt, wird der Firewall-Administrator per E-Mail informiert.

Fazit Firmware-Updates

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Hersteller führt Fehlerkorrekturen durch und stellt die neue Firmware auf seiner Homepage zum Download zur Verfügung
- Download der aktuellen Firmware von der Hersteller-Homepage problemlos möglich
- Update lässt sich effizient und ohne Schwierigkeiten über einen entsprechenden Konfigurations-Menupunkt einspielen
- Firewall-Administrator hat die Möglichkeit, sich bei Vorliegen einer neuen Firmware-Version automatisch informieren zu lassen

⊖

6.3.14 Backup und Restore der Firewall-Konfiguration

Die Firewall-Konfiguration (inkl. aller Einstellungen zu den Zusatzfunktionalitäten) lässt sich über das Web-GUI sichern und bei Bedarf wiederherstellen. Ausserdem kann die Firewall auf ihre Werkeinstellungen zurückgesetzt werden.

Fazit Backup und Restore der Firewall-Konfiguration

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Alle Einstellungen lassen sich in einer Backup-Datei sichern, welche bei Bedarf ohne Probleme wieder zurückgespielt werden kann

⊖

6.3.15 Hohe Verfügbarkeit

Die Firewall verfügt über den Menupunkt „High Availability“, über welchen die Verbindung zu einer zweiten SonicWALL-Firewall eingerichtet werden kann. Dabei muss die Seriennummer und die IP-Adresse der Backup-Firewall hinterlegt werden. Die beiden Firewalls müssen sich im gleichen lokalen Netzwerksegment befinden. Die Firewalls verwenden ein so genanntes „Heartbeat“-Signal, um miteinander zu kommunizieren. Wenn die Backup-Firewall während einer frei definierbaren Zeit kein Signal mehr von der primären Firewall erhält, übernimmt sie die Funktion der primären Firewall. Ansonsten befindet sich die Backup-Firewall im Leerlauf. Konfigurationsänderungen, welche an der primären Firewall vorgenommen werden, werden

automatisch auf die Backup-Firewall synchronisiert. Der Synchronisationsvorgang kann jedoch jederzeit auch manuell gestartet werden.

Fazit hohe Verfügbarkeit

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Wie der Name bereits sagt, kann auf diese Weise die Verfügbarkeit der Firewall-Infrastruktur und letztlich des Netzwerkübergangs vom LAN ins WAN und umgekehrt hoch gehalten werden
- SonicWALL ist für das Einrichten einer Hochverfügbarkeitslösung bestens vorbereitet. Es müssen keine weiteren (Dritt-)Produkte angeschafft werden

⊖

6.3.16 Schutz der Firewall vor Angriffen

Die Firewall bietet eine „Randomize IP ID"-Option an, bei welcher die IP-Pakete der Firewall mit einer zufälligen IP-ID versehen werden, um einem potentiellen Angreifer die Identifikation der Firewall zu erschweren. Ausserdem lässt sich ebenfalls der so genannte „Stealth Modus" aktivieren, um die Firewall vor möglichen Angriffen sicherer zu machen.

Eine Portscanning-Analyse unter Mithilfe eines Sniffers führte dabei zu folgenden Resultaten:

Durchgeführter Test	*Firewall-Interface*	*Stealth-Modus aktiv?*	*Von der Firewall erhaltene Resultate*
Portscan aus dem WAN gegen die Firewall auf nicht verwendete Ports	Extern	Nein	Firewall antwortet mit einem Reset- und Acknowledgment-Paket (RST/ACK) / Ports werden vom Portscanner als „geschlossen" bezeichnet
Portscan aus dem WAN gegen die Firewall auf nicht verwendete Ports	Extern	Ja	Keine Antwort von der Firewall / Ports werden vom Portscanner als „gefiltert" bezeichnet
Portscan aus dem LAN gegen die Firewall auf nicht verwendete Ports	Intern	Nein	Firewall antwortet mit einem Reset- und Acknowledgment-Paket (RST/ACK) / Ports werden vom Portscanner als „geschlossen" bezeichnet
Portscan aus dem LAN gegen die Firewall auf nicht verwendete Ports	Intern	Ja	Firewall antwortet mit einem Reset- und Acknowledgment-Paket (RST/ACK) / Ports werden vom Portscanner als „geschlossen" bezeichnet

Tabelle 19: SonicWALL SOHO3 – Resultate Portscans mit Firewall-Stealth-Modus

Bei aktiviertem Stealth-Modus ändert sich das Antwortverhalten der Firewall auf Portscans lediglich auf dem externen WAN-Interface. Der Stealth-Modus schützt jedoch nicht vor Firewall-Angriffen aus dem internen Netzwerk.

Fazit Schutzmechanismen

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Bei aktiviertem Stealth-Modus antwortet die Firewall bei Portscans aus dem WAN / Internet nicht mehr. Dies erschwert die Arbeit eines möglichen Angreifers

⊖

- Der Stealth-Modus ist nur auf dem externen, jedoch nicht auf dem internen Interface wirksam

6.3.17 Logische Netzwerksegmente

Die Firewall unterstützt über ihr physisches LAN-Interface weitere logische LAN-Interface und somit auch weitere logische Netzwerksegmente. Der Verkehr zwischen den logischen LAN-Segmenten passiert zwar die Firewall (diese nimmt ja zwingend auch das Routing vor), es war jedoch nicht möglich, diesen Netzwerkverkehr durch Firewall-Regeln einzuschränken. Der Zugriff aus einem logischen Netzwerksegment in ein anderes logisches Netzwerksegment ist somit uneingeschränkt möglich.

Fazit logische Netzwerksegmente

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☹

⊕

- Das interne Netzwerk (LAN) kann auf einfache Art und Weise segmentiert werden

⊖

- Firewall-Regeln lassen sich zwischen den logischen Segmenten nicht konfigurieren, wodurch der Verkehr nicht gezielt kontrolliert werden kann; eine Abschottung der Systeme zwischen den logischen Netzwerksegmenten ist somit nicht möglich

6.3.18 WAN-Protokolle

Die Firewall unterstützt mittels PPPoE (Point-to-Point Protocol over Ethernet) eine direkte Verbindung zu einem Breitbandmodem (z.B. für eine Anbindung an einen ADSL-ISP). Dabei können die Zugangsdaten (Benutzername, Passwort) für den ISP direkt auf der Firewall eingegeben und gespeichert werden.

Zudem werden die Protokolle L2TP (Layer 2 Tunneling Protocol) und PPTP (Point-to-Point Tunneling Protocol) für eine Anbindung an einen ISP unterstützt. Auf diese Weise kann ein verschlüsselter VPN-Zugang zum ISP eingerichtet werden.

Fazit WAN-Protokolle

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs -

⊕

- Die Benutzerinformationen für einen Internet-Breitbandzugang wie z.B. ADSL lassen sich direkt auf der Firewall hinterlegen
- Mit den Protokollen PPTP und L2TP können verschlüsselte Internet-Provider-Zugänge, falls von den Internet-Providern unterstützt, hergestellt werden

⊖

7. CHECK POINT FIREWALL-1 NEXT GENERATION

7.1 Allgemeine Hinweise zur Firewall

Bei der Check Point Firewall-1 NG handelt es sich um ein Software-Produkt, welches unter verschiedenen Betriebssystemen installiert werden kann. Als Betriebssysteme kommen dabei Standardbetriebssysteme wie Windows NT 4.0 oder Windows 2000 Server, Sun Solaris 8 oder 9 und Red Hat Linux aber auch proprietäre Betriebssysteme wie Nokia IPSO und Check Point SecurePlatform in Frage. Falls das Produkt auf einem Standardbetriebssystem installiert wird, muss sich der Firewall-Administrator um die Härtung des Betriebssystems (d.h. das Absichern des Betriebssystems um zu verhindern, dass allfällige Schwachstellen des Betriebssystems die Schutzwirkung und Gesamtsicherheit der Firewall beeinträchtigen) kümmern. Bei den proprietären Betriebssystemen wurde die Härtung normalerweise bereits durch den Hersteller vorgenommen.

Die Check Point Firewall zielt aufgrund ihrer Komplexität und Vielfältigkeit, jedoch auch aufgrund ihres Preises, auf grössere KMU und Grossbetriebe ab. Auch der Aufwand für den Unterhalt der Firewall darf nicht unterschätzt werden; gilt es doch, je nach installierter Variante, sowohl ein Betriebssystem als auch die Firewall selbst auf dem aktuellen Stand zu halten, um ein möglichst hohes Sicherheitsniveau zu erreichen.

Die Firewall arbeitet ebenfalls nach dem „Stateful Inspection"-Prinzip (die Firma Check Point ist der Erfinder dieses Prinzips) und setzt zusätzlich, je nach Konstellation, so genannte „Security Servers" ein. Dabei handelt es sich um eine Art Application-Gateway, da die Verbindung von der Quelle zum Ziel durch die Firewall unterbrochen wird, d.h. es bestehen zwei Verbindungen, nämlich eine Verbindung von der Quelle auf die Firewall und eine Verbindung von der Firewall zum Ziel. Auf diese Weise kann die Firewall den Verkehr besser kontrollieren und es lassen sich Authentisierungsmechanismen einsetzen.

Die Anzahl der vorhandenen Firewall-Interface ist grundsätzlich abhängig von den hardwaremässig installierten und durch das Betriebssystem erkannten Netzwerkkarten resp. Netzwerk-Interface. Falls die Server-Hardware genügend Platz bietet, kann auch zu einem späteren Zeitpunkt die Anzahl der Interfaces problemlos erweitert werden (im Unterschied zu den integrierten Firewall-Lösungen wie ZyWALL oder SonicWALL, bei welchen eine nachträgliche Erweiterung nicht vorgesehen ist).

Die Administration der Firewall erfolgt entweder über die Command-Shell oder über die grafischen „Check Point Smart Clients", welche entweder auf der Firewall selber oder aber auf einem Firewall-Administrationsarbeitsplatz irgendwo im Netzwerk ausgeführt werden.

Die während dieser Diplomarbeit gewonnen Erkenntnisse zu den Zusatzfunktionalitäten der Check Point Firewall-1 NG basieren alle auf den zu diesem Zeitpunkt aktuellen Software-Releases für die „Windows 2000-Variante" der Firewall (Check Point Firewall-1 NG Feature Pack 3 mit SVN Foundation Build 53965, FW-1 und VPN-1 Build 53945 und SMART Client Build 53933). Es gilt jedoch zu berücksichtigen, dass im Rahmen dieser Diplomarbeit nicht alle von Check Point erhältlichen Module bzw. Erweiterung installiert und bezüglich ihrer Zusatzfunktionalitäten untersucht wurden. Gegenstand der Analysen und Tests waren die Module VPN-1 & Firewall-1, Smart Clients und Policy Server. Andere Elemente wie FloodGate-1, User Authority, SmartView Monitor, SmartView Reporter, Provider-1/SiteManager-1 und

VPN-1 Acceleration bleiben in den folgenden Ausführungen unberücksichtigt. Ausserdem lässt die Fülle der Optionen dieser Firewall eine Analyse aller angebotenen Zusatzfunktionen bis ins Detail im Rahmen dieser Diplomarbeit nicht zu. Der Autor hat sich deshalb auf die wesentlichsten Zusatzfunktionalitäten, wie sie in Kapitel 2 generisch umschrieben wurden, konzentriert.

Zum Testen der Firewall-Zusatzfunktionalitäten wurde folgende Versuchsumgebung aufgebaut, wobei die Installation aller verfügbarer Check Point Module zentral auf einem System erfolgte:

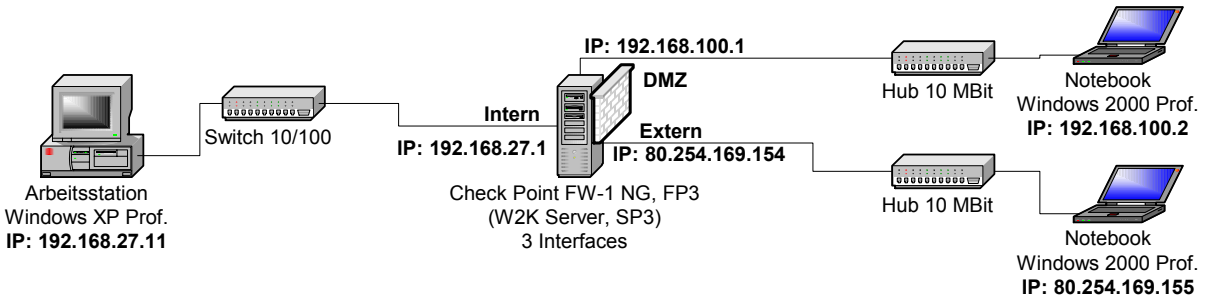


Abbildung 24: Check Point Firewall-1 NG – Versuchsumgebung für die Durchführung der Firewall-Tests

Die Windows XP Arbeitsstation und das Windows 2000 Notebook waren mit diversen Tools (Portscanner, Sniffer usw.) ausgestattet, um die technischen Tests möglichst umfassend durchführen zu können. Das Notebook konnte wahlweise an einem der Hubs angeschlossen werden.

7.2 Grundkonfiguration und wesentliche Standardeinstellungen

Wie in der Abbildung 24 ersichtlich ist, wurde die Firewall auf einem Windows 2000 Server Betriebssystem installiert. Damit die Firewall das Routing zwischen den einzelnen Interface vornehmen kann, muss dieses auf Betriebssystemebene vorgängig aktiviert werden. Auf dem Windows 2000 Server erfolgt diese Einstellungen in der Systemsteuerung unter „Routing and Remote Access“.

Nach der Installation der Firewall-Software muss das System neu gestartet werden. Da während des Startvorgangs des Betriebssystems der Firewall-Schutz noch nicht greifen kann, hat Check Point eine so genannte „Boot Security“ implementiert. Diese soll während des Systemstarts sowohl die Firewall selber als auch die internen Netzwerke hinter der Firewall schützen. Bei „Boot Security“ handelt es sich insbesondere um folgende Elemente:

- Kontrolle des Routing (IP Forwarding) während des Bootvorgangs, d.h. dass das Routing während des Bootvorgangs deaktiviert wird. Dies dient dem Schutz der internen Netzwerke hinter der Firewall
- Aktivierung eines Standard-Firewall-Filters während des Bootvorgangs zum Schutz der Firewall selber und der internen Netzwerke hinter der Firewall. Der Standard-Filter erlaubt alle ausgehenden Verbindungen und schützt vor Anti-Spoofing, eingehende Verbindungen werden hingegen keine zugelassen

- Aktivierung einer Initial-Policy mit impliziten Firewall-Regeln, damit die Sicherheits-Policy (das Regelwerk der Firewall) nach dem Systemstart angelegt werden kann. Sobald eine Sicherheits-Policy auf der Firewall angelegt wurde, kommt die Initial-Policy bei weiteren Systemstarts nicht mehr zur Anwendung

Nach dem Systemstart kann mittels „Check Point SmartDashboard“ auf die Firewall zugegriffen werden um die Sicherheits-Policy zu definieren und danach auf der Firewall zu installieren.

Standardmässig aktivierte Einstellungen, wie dies bei der ZyWALL und SonicWALL der Fall war, gibt es bei der Check Point Firewall nach dem ersten Systemstart grundsätzlich nicht. Alle Einstellungen (von den Administratoren, Benutzern, Interfaces bis hin zu den Objekten und Regelwerken) müssen durch den Firewall-Administrator selber erstellt oder zumindest aktiviert werden.

Durch die Komplexität der Firewall können bei der Installation oder beim erstmaligen Systemstart unter Umständen bereits Probleme auftreten. Check Point liefert mit ihrem Produkt zwar mehrere umfangreiche elektronische Handbücher für die verschiedenen Module aus. Diese sind jedoch zum Teil unvollständig bzw. nicht auf dem neusten Stand sowie teilweise stark fehlerbehaftet und deshalb nur bedingt für die rasche gezielte Problemlösung geeignet. So wird z.B. im „Getting Started Guide“ zwar erwähnt, dass auf Betriebssystemebene das IP-Forwarding (Routing) aktiviert werden soll, es wird jedoch nur aufgezeigt, wie diese Einstellung unter Windows NT Server vorgenommen werden kann. Über Windows 2000 Server schweigt sich das Handbuch diesbezüglich aus, obwohl die Einstellung unter Windows 2000 Server an einem komplett anderen Ort als unter Windows NT 4.0 vorgenommen werden muss.

<u>Fazit Grundkonfiguration und wesentliche Standardeinstellungen</u>

Beurteilung der Grundkonfiguration bezüglich Aufwand, Verständlichkeit usw. 😐

Auswirkungen der Grundkonfiguration auf die Gesamtsicherheit der Firewall ☺

⊕

- Die Firewall und die internen Netzwerke sind nach der Firewall-Installation und beim Systemstart durch die „Boot Security“-Mechanismen vor unberechtigten Zugriffen geschützt
- Die Firewall muss zuerst aktiv durch einen Firewall-Administratoren konfiguriert werden, bevor auf interne Systeme zugegriffen werden kann

⊖

- Handbücher sind zum Teil unvollständig resp. veraltet und/oder stark fehlerbehaftet

7.3 Zusatzfunktionalitäten

Die Zusatzfunktionalitäten der Firewall werden im folgenden Kapitel grundsätzlich in der gleichen Reihenfolge, in der sie in Kapitel 2 generisch umschrieben wurden, abgehandelt.

Da es sich bei der Check Point Firewall-1 NG primär um ein Softwareprodukt handelt, welches auf einem vollwertigen Betriebssystem basiert, können einige der in den vorhergehenden Kapiteln erwähnten und bei den beiden anderen getesteten Firewalls explizit genannten Zusatzfunktionalitäten direkt durch das Betriebssystem abgedeckt werden (z.B. DHCP-Server, Zeitserver-Dienst usw.). Falls die Firewall eine der in Kapitel 2 erwähnten Zusatzfunktionalitäten nicht unterstützt oder die Funktionalität durch das zugrunde liegende Betriebssystem abgedeckt wird, wird sie in diesem Kapitel nicht aufgeführt (es erfolgt somit kein expliziter Hinweis, dass die entsprechende Funktionalität nicht zur Verfügung steht oder bereits durch das Betriebssystem abgedeckt wird; eine solche Gesamtübersicht mit entsprechenden Hinweisen folgt in Kapitel 8).

Es gilt zudem zu berücksichtigen, dass die Konfiguration einiger in Kapitel 2 erwähnten Zusatzfunktionalitäten auf der Firewall jeweils an ein und derselben Stelle bzw. im gleichen Menu erfolgt. In einem solchen Fall werden diese Zusatzfunktionalitäten auch im vorliegenden Kapitel entsprechend zusammengefasst.

7.3.1 Authentisierungsmöglichkeiten

Die Check Point Firewall-1 NG unterstützt drei Authentisierungstypen mit verschiedenen Authentisierungsschemen. Bei den Authentisierungstypen (siehe Abbildung 25) handelt es sich um:

User Authentication	Die Authentisierung erfolgt benutzerbasiert und kann für die Dienste Telnet, FTP, rlogin und HTTP eingesetzt werden. Für jede Verbindung ist eine separate Authentisierung erforderlich
Session Authentication	Auch bei dieser Variante ist für jede Verbindung eine separate Authentisierung erforderlich. Sie kann jedoch für alle Dienste eingesetzt werden und unterliegt nicht den Dienste-Einschränkungen der User Authentication. Um diese Authentisierungsvariante einzusetzen, muss jedoch der so genannte „Session Authentication Agent“ auf dem Client oder einem anderen System im Netzwerk installiert sein
Client Authentication	Der Zugriff wird systembasierend gewährt. Diese Variante unterstützt alle Verbindungen von einer spezifischen IP-Adresse nach erfolgreicher Authentisierung. Sie kann für beliebig viele Verbindungen und für alle Dienste eingesetzt werden

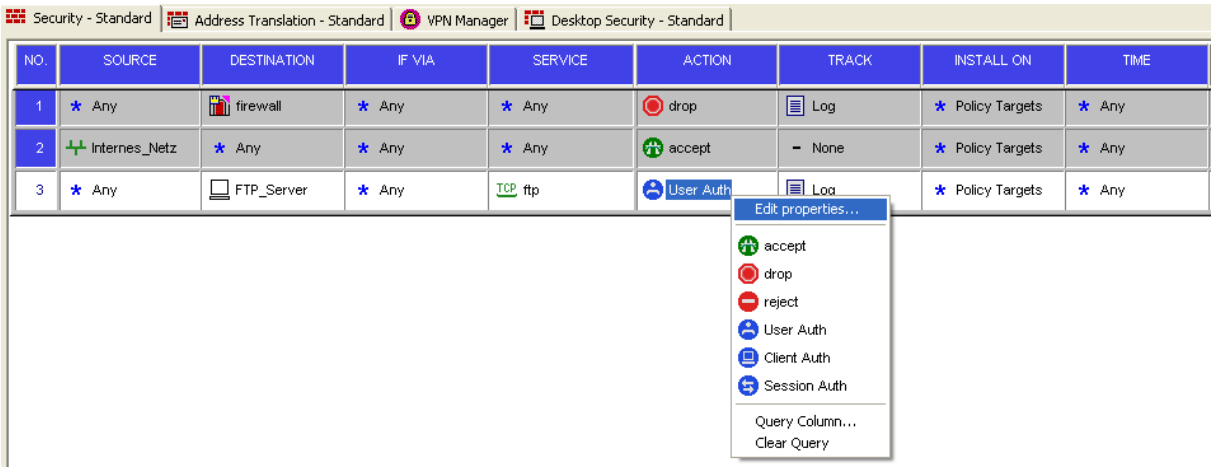


Abbildung 25: Check Point Firewall-1 NG – Auswahl des Authentisierungstyps pro Firewall-Regel

Zwischen folgenden Authentisierungsschemen kann gewählt werden:

S/Key	Zur Anmeldung wird ein Einmalpasswort (one-time password) basierend auf einer Einweg-Hashfunktion verwendet
SecurID	Zur Anmeldung wird eine SecurID-Karte benötigt
OS Password	Verwendung des Betriebssystempassworts
VPN-1 & Firewall-1 Password	Zur Anmeldung wird das auf der Firewall erfasste Benutzer-Passwort benötigt
RADIUS	Anmeldung basiert auf den Benutzerdaten eines Radius-Servers
Axent Pathways	Anmeldung basiert auf den Benutzerdaten eines Axent Pathways-Servers
TACACS	Anmeldung basiert auf den Benutzerdaten eines TACACS oder TACACS+-Servers
Undefiniert	Es wird keine Authentisierung durchgeführt und der Zugriff wird immer verwehrt

Mit Hilfe dieser Authentisierungsmöglichkeiten können Zugriffe auf frei definierbare Zielsysteme und Dienste sowohl vom internen Netzwerk ins externe Netzwerk/Internet als auch vom externen Netzwerk ins interne Netzwerk eingeschränkt werden.

Die erfassten Benutzer können zu Gruppen zusammengefasst werden und je Benutzer lässt sich festlegen, zu welchen Zeiten und an welchen Wochentagen er eine authentisierte Verbindung aufbauen darf.

Die Anmeldeinformationen werden standardmässig unverschlüsselt (siehe Abbildung 26) über das Netzwerk übermittelt. Für die Varianten Session- und Client-Authentication kann jedoch eine SSL-Verschlüsselung definiert und aktiviert werden. Danach erfolgt die Übermittlung der Benutzerinformationen verschlüsselt (siehe Abbildung 27).

```
220 FW-1 Session Authentication Request from firewall
211 1358866843 1184 3232242442 21 6
331 User:
test331 *password:
versuch200 User test authenticated by FireWall-1 authentication.
230 OK
```

Abbildung 26: Check Point Firewall-1 NG – Unverschlüsselte Session-Authentisierung

```
220 FW-1 Session Authentication Request from firewall
201 131072
211 1358866843 1182 3232242442 21 6
331 User:
□□□□131072202
□□U□Q□>Ì™ý¦,FPI'‡¥A□□š ¬ZŸ¶Š '®`Ò8ÕsR† ¥□ê□ æ□)e5·«_□¦@.¦J;ø1¯€´'AŒEÍk□
□□□□□□□□J□F□>ÌšLý□ú<?v\°r~□®P□□N'%ç□¥%ø¯öÏ)Ý Jiü@□a&ÇŽÚ®Ç-□i□fHdöÖš_M□ □f□ýÃ□□□□□□□□€
E□□|^³□|[-Žöó□É#ÀC8¥[□□Ž»U□E¸]8Ó4ý|□WC£□□l□3!,µ*ÿ<á±)@□□□|„§
rÖ†Ä□□È□)zÊ▪□Ù-Ÿ«Ð
P›□FÓ□=f¤]AŸœ|½%K"□&°«¢^ÃUé/xÇ□□€ÇÔã®Ñ¶□o□¹™O6□@¼ei8□%Ø< ‡□†dßq5w□□±´n|″Å´Xšù£□M@×äK§.ò
©Ý°õÁôfF□□□□□□†□,€WŸ_æ□Ñ÷Ér°`ãc±5□è□ƒka□ú%Ùz=D□qô□N□Ð□÷ßú~¡žõõü™″JZsòæÑ□×'Ÿé†Œ±ž²□I
"Ä°Ô¨Än¦µã□ÆÆY·□©□ò□ô—□□ -8Ë-□″-□Ég˜Íéi□\¸8É
□›Ü%?ÜÐÅõ£«□□(°Î){³ŸpË□Ry□Ò□ü□□³¼□³®.-ÀZ7Wý¡°″□ ßV¢@□a□□ ¼_(□□o"¥l □dŸžŠÐ<EÊ□U¯ždë¿õ3
s+□[õÅß□□†□y□@»ÿ´7/[□b1=ý″û\Opa³z□4[Âèi□□ Xk-□□
□ç},7×□µ¼□}¦á`
½hŸJ¼=8□y&9□□□à×#À□□□¹^ZGÛHÖ"ÅQ²,x~D~□□□□÷QägýÅ□û□□7]Þv³□šÀ"¨GNi□
```

Abbildung 27: Check Point Firewall-1 NG – Mit SSL verschlüsselte Session-Authentisierung

Die Authentisierung erfolgt je nach gewähltem Verfahren transparent oder nicht transparent. Bei der transparenten Authentisierung stellt der Benutzer direkt eine Verbindung zum gewünschten Ziel-System her; die Firewall fordert ihn automatisch dazu auf, sich zuerst auf der Firewall zu authentisieren. Bei der nicht transparenten Authentisierung muss sich der Benutzer zuerst explizit auf der Firewall authentisieren bevor er eine Verbindung zum gewünschten Zielsystem aufbauen kann.

Fazit Authentisierungsmöglichkeiten

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Ein Benutzer erhält erst Zugriff auf einzelne Bereiche oder Funktionen nachdem er sich erfolgreich authentisiert hat
- Gezielte Freigaben für Zugriffe aus dem WAN aufs LAN und aus dem LAN aufs WAN möglich
- Unterstützung von sehr vielen Authentisierungstypen und Authentisierungsschemen; sehr hohe Flexibilität

⊖

- Unterstützung von Verschlüsselung der Benutzerinformationen (Benutzername und Passwort) bei der Anmeldung

7.3.2 Zeiteinschränkung einzelner Firewall-Regeln

Pro Zeiteintrag lassen sich drei Zeitperioden (von/bis) definieren. Diese Zeitperioden gelten entweder für jeden Tag, für bestimmte Tage einer Woche oder für frei definierbare Tage eines bestimmten Monats oder jedes Monats eines Jahres. Einer Firewall-Regel lassen sich beliebig viele solche Zeiteinträge zuordnen. Ausserdem können die Zeiteinträge auch in Zeitgruppen zusammengefasst werden, um die Übersichtlichkeit zu erhöhen.

Die Konfigurationsmöglichkeiten im Rahmen der Zeiteinschränkungen sind somit äusserst flexibel und lassen keine Wünsche offen.

Fazit Zeiteinschränkungen einzelner Firewall-Regeln

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs

- Firewall-Regeln können zeitlich beliebig und äusserst flexibel eingeschränkt werden; auf diese Weise können bestimmte Aktivitäten (z.B. Wartungszugriffe, externe Partner-Zugriffe usw.) gezielt gesteuert und besser überwacht und kontrolliert werden

7.3.3 Content-, SMTP- und URL-Filtering

Mit Hilfe der so genannten „Security Servers“ von Check Point kann für einige Dienste neben der Authentisierung (siehe dazu auch Kapitel 7.3.1) ein Content-Filtering implementiert werden. Folgende Tabelle gibt einen Überblick über die Eigenschaften der Security Servers und der Content-Filtering-Möglichkeiten der einzelnen Dienste:

Dienst	***Authentisierung***	***Content-Filtering***	***Erläuterungen zum Content-Filtering***
Telnet	Ja	Nein	-
rlogin	Ja	Nein	-
FTP	Ja	Ja	Content-Filtering basierend auf den Befehlen „put“ und „get“ und Dateinamen- bzw. Pfadrestriktionen (siehe Abbildung 28). Überprüfung auf Viren mittels Drittprodukt.

HTTP	Ja	Ja	Content-Filtering basierend auf den Protokollen HTTP, FTP, GOPHER usw. und auf den Methoden GET, POST, usw.; Domäneneinschränkungen und Einschränkungen im Bereich des Pfades; Java-Applets können geblockt werden.
SMTP	Nein	Ja	Content-Filtering basierend auf dem Absender und Empfänger des E-Mails; Einschränkungen aufgrund des Attachment-Typs (siehe Abbildung 29); Implementation von Secure Sendmail um direkte Attacken auf den Sendmail-Server zu verhindern.

Tabelle 20: Check Point Firewall-1 NG – Eigenschaften der Security Server

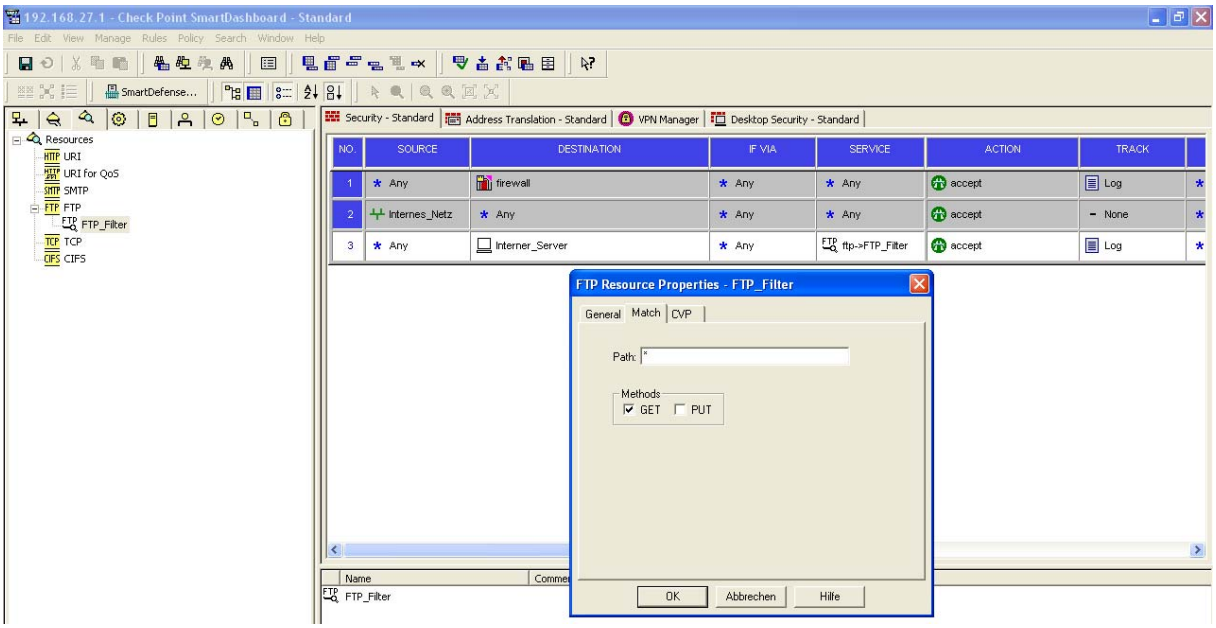


Abbildung 28: Check Point Firewall-1 NG – Content-Filtering beim FTP-Dienst

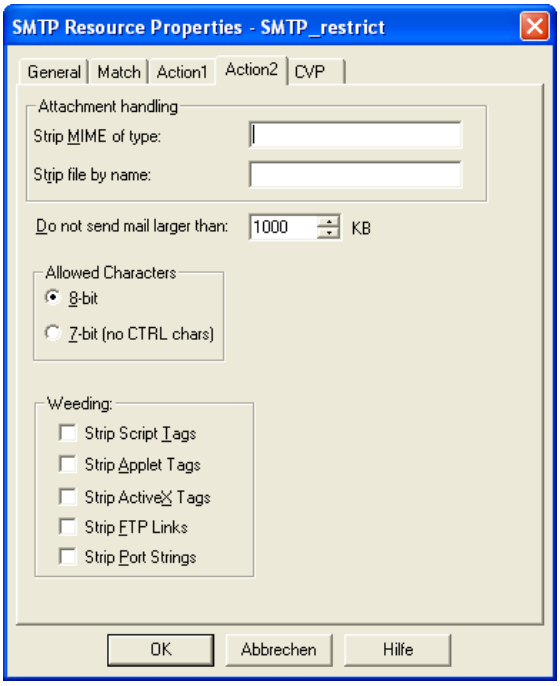


Abbildung 29: Check Point Firewall-1 NG – SMTP-Filtering aufgrund des Attachment-Typs

Um den Inhalt der Datenpakete auf Viren zu überprüfen, ist die Anbindung einer Anti-Virensoftware eines Drittherstellers möglich. Die Anbindung erfolgt dabei über das so genannte „Content Vectoring Protocol“ (CVP) und über die standardisierte OPSEC-Schnittstelle.

Ein umfassendes URL-Filtering ist nicht direkt auf der Firewall implementiert. Falls ein solches vorgenommen werden soll, ist eine Anbindung an einen entsprechenden URL-Filtering-Server eines Drittherstellers über das „URL Filtering Protocol“ (UFP) notwendig. Diese Anbindung erfolgt ebenfalls über die standardisierte OPSEC-Schnittstelle.

Fazit Content-, SMTP- und URL-Filtering

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Die Firewall verfügt über ein Content-Filtering für die Dienste FTP, HTTP und SMTP. Im Bereich des HTTP-Filterings können auch Java-Applets geblockt werden
- Durch das SMTP-Filtering können Sendmail-Server hinter der Firewall geschützt werden (direkte Verbindungen auf den Sendmail-Server werden durch die Firewall verhindert)
- Die Filtereinstellungen pro Dienst können teilweise auf einzelnen Firewall-Regeln oder aber für den Dienst als solches aktiviert werden

⊖

- Direkt auf der Firewall ist kein umfassendes URL-Filtering implementiert. Falls ein solches gewünscht wird, muss auf Produkte von Drittherstellern zurückgegriffen werden

- Die Firewall unterstützt die Anbindung an Content- und URL-Filtering-Software (inkl. Anti-Virenprogramme) von Drittherstellern
- Auch wenn direkt auf der Firewall lediglich Content-Filtering, jedoch kein URL-Filtering angeboten wird, trägt diese Funktionalität zu einer höheren Gesamtsicherheit der Firewall und der internen Netzwerke bei

7.3.4 „Intrusion Detection"-Funktionen, Anti-Spoofing

Die „Intrusion Detection"-Funktion unter Check Point Firewall-1 NG nennt sich SmartDefense. Mit SmartDefense lassen sich Attacken aufgrund ihres Typus und ihrer Klasse blocken. Allfällige DoS- (Denial of Service) und andere Attacken sollen damit möglichst frühzeitig erkennt und geloggt werden. In SmartDefense können unter anderem Einstellungen zur Erkennung folgender Attacken vorgenommen werden (siehe Abbildung 30):

- DoS-Attacken
  - Ping of Death
  - SYN flooding
  - Land
  - Teardrop
- IP Spoofing auf LAN- und WAN-Interface
- Portscans
- Erhalt von IP-Paket-Fragmenten
- Erhalt von IP-Paketen mit nicht konformem Inhalt oder unsinnigen Header-Informationen
- HTTP-Würmer (Angriffe auf Web-Server wie z.B. CodeRed oder Nimda)

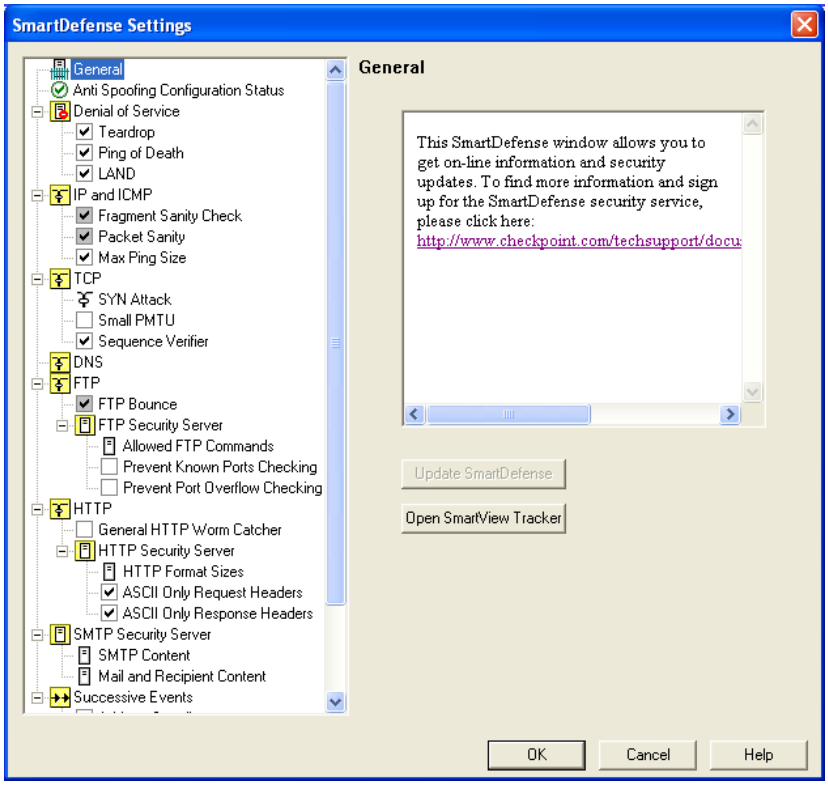


Abbildung 30: Check Point Firewall-1 NG – SmartDefense-Einstellungsmöglichkeiten

Die „Intrusion Detection"-Funktion lässt sich kontinuierlich aktualisieren, damit z.B. auch neue HTTP-Würmer erkannt werden. Für diese Dienstleistung wird jedoch eine separate kostenpflichtige Lizenz benötigt.

Das IP-Spoofing (siehe Abbildung 31) auf dem externen und den internen Interface der Firewall und alle durchgeführten Portscan-Attacken[43] sowohl aus dem internen als auch aus dem externen Netzwerk auf die Firewall wurden korrekt durch die Firewall registriert und aufgezeichnet, wobei spezielle Portscan-Varianten wie z.B. FIN- oder XMAS-Scans aufgrund ihrer nicht standesgemässen TCP-Flags durch SmartDefense verworfen und geblockt wurden (siehe Abbildung 32). Die Schwellenwerte zur Erkennung von Attacken können für die meisten Ereignisse durch den Firewall-Administrator frei definiert werden. Einige der „Intrusion Detection"-Funktionen wie z.B. die Erkennung von Portscans, von Local Interface Spoofing usw. basieren auf der Log-Datei der Firewall, d.h. dass SmartDefense die aufgezeichneten Log-Einträge analysiert und aufgrund dessen Alarme auslöst. Es ist deshalb zwingend, die entsprechenden Vorkommnisse zu loggen, da sonst die „Intrusion Detection"-Funktion ihre Aufgabe nicht vollumfänglich wahrnehmen kann.

[43] Die Portscans wurden mit dem Programm „nmap" durchgeführt (www.insecure.org)

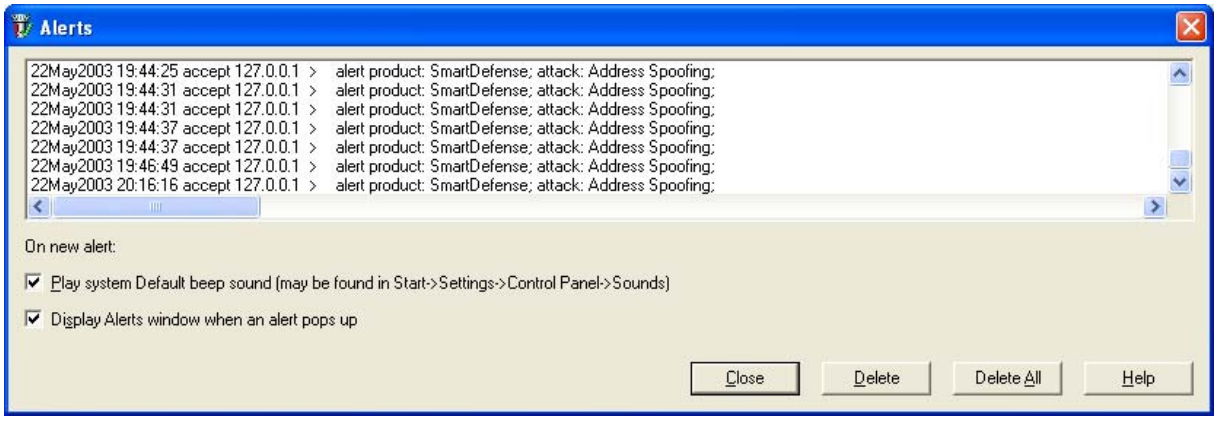

Alerts
22May2003 19:44:25 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
22May2003 19:44:31 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
22May2003 19:44:31 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
22May2003 19:44:37 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
22May2003 19:44:37 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
22May2003 19:46:49 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
22May2003 20:16:16 accept 127.0.0.1 > alert product: SmartDefense; attack: Address Spoofing;
On new alert:
Play system Default beep sound (may be found in Start->Settings->Control Panel->Sounds)
Display Alerts window when an alert pops up
Close
Delete
Delete All
Help

Abbildung 31: Check Point Firewall-1 NG – Erkennung und Alarmierung von IP-Spoofing

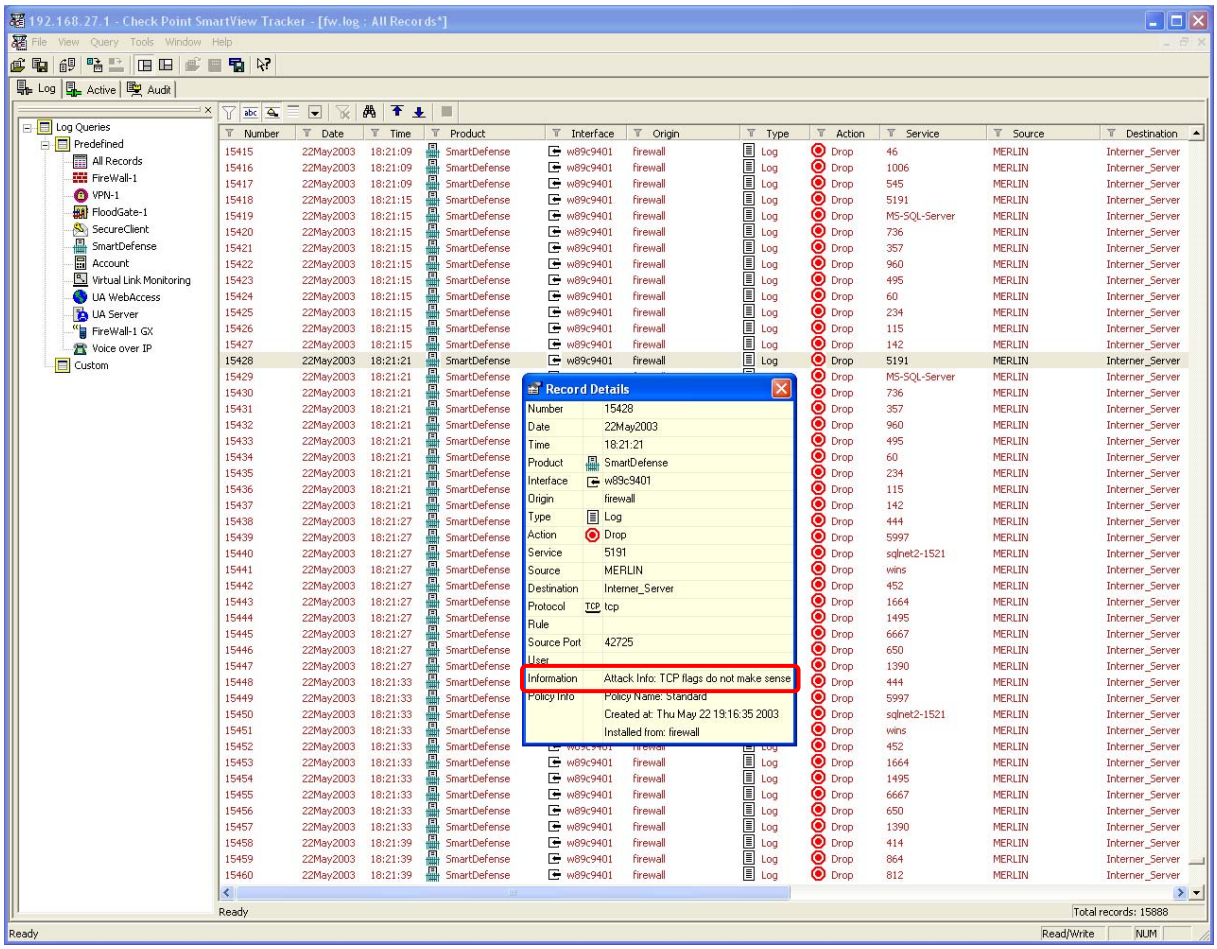


Abbildung 32: Check Point Firewall-1 NG – Blocken von Paketen aufgrund ihrer TCP-Flags

Ausserdem wurde der Zugriff auf einen Web-Server im internen Netzwerk bei der Eingabe von URLs, welche Elemente der in der Filter-Liste definierten HTTP-Würmer (Test mit Nimda-Wurm) beinhalteten, erfolgreich von der Firewall geblockt. Die Abwehr der so genannten HTTP-Würmer funktioniert somit wie vorgesehen.

Fazit „Intrusion Detection"-Funktion, Anti-Spoofing

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Die Firewall erkennt allfällige DoS- oder andere Attacken zuverlässig und alarmiert den Firewall-Administrator unmittelbar mittels Alarm, Mail oder SNMP-Trap
- Portscans sowohl auf das externe als auch die internen Interface der Firewall werden als solche unabhängig vom gewählten Verfahren erkannt
- IP-Spoofing wird sowohl auf den internen als auch auf dem externen Interface der Firewall erkannt
- Web-Server lassen sich aufgrund der HTTP-Wurm-Erkennung schützen
- Die Schwellenwerte der meisten Ereignisse lassen sich frei definieren. Dadurch können sowohl „False Postitive"- als auch „False Negative"-Meldungen reduziert werden

⊖

7.3.5 Erweiterte Logging-Möglichkeiten und Alarmierung

Bei jeder Firewall-Regel kann gewählt werden, ob die Vorkommnisse, welche diese Regel betreffen, nicht festgehalten, geloggt, alarmiert (an Systemkonsole), an einen Systemmanagement-Server (SNMP-Trap) gesendet, per E-Mail versendet oder benutzerdefiniert abgehandelt werden sollen. Für die Alarmierung von „Intrusion Detection"-Vorkommnissen stehen die gleichen Alarmierungsmöglichkeiten zur Verfügung (siehe dazu auch Kapitel 7.3.4).

Zur Einsicht in die Log-Datei muss der „SmartView Tracker" gestartet werden. Die Informationen in der Log-Datei sind sehr umfangreich; standardmässig werden angezeigt: Datum; Uhrzeit; Produkt, welches den Log-Eintrag veranlasst hat; betroffenes Interface; Herkunft; Typ der Aufzeichnung; Information, ob Paket akzeptiert oder verworfen wurde; Ziel-Port; Quellsystem; Zielsystem; Protokoll; betroffene Firewall-Regel; Quell-Port; Benutzer; weitere Informationen.

Die Bildschirmausgabe der Log-Datei lässt sich beliebig anpassen. Insgesamt werden ungefähr 110 Parameter in der Log-Datei aufgezeichnet. Jeder dieser Parameter kann als eigenständige Spalte in der Tabelle ausgegeben werden (siehe Abbildung 33). Der Firewall-Administrator kann für die Werte jeder Spalte einen Filter setzen. Diese Filter können kumulativ eingesetzt werden. Auf diese Weise lassen sich die gewünschten Informationen schnell anzeigen. Ausserdem besteht die Möglichkeit, über alle Spalten hinweg nach Einträgen zu suchen.

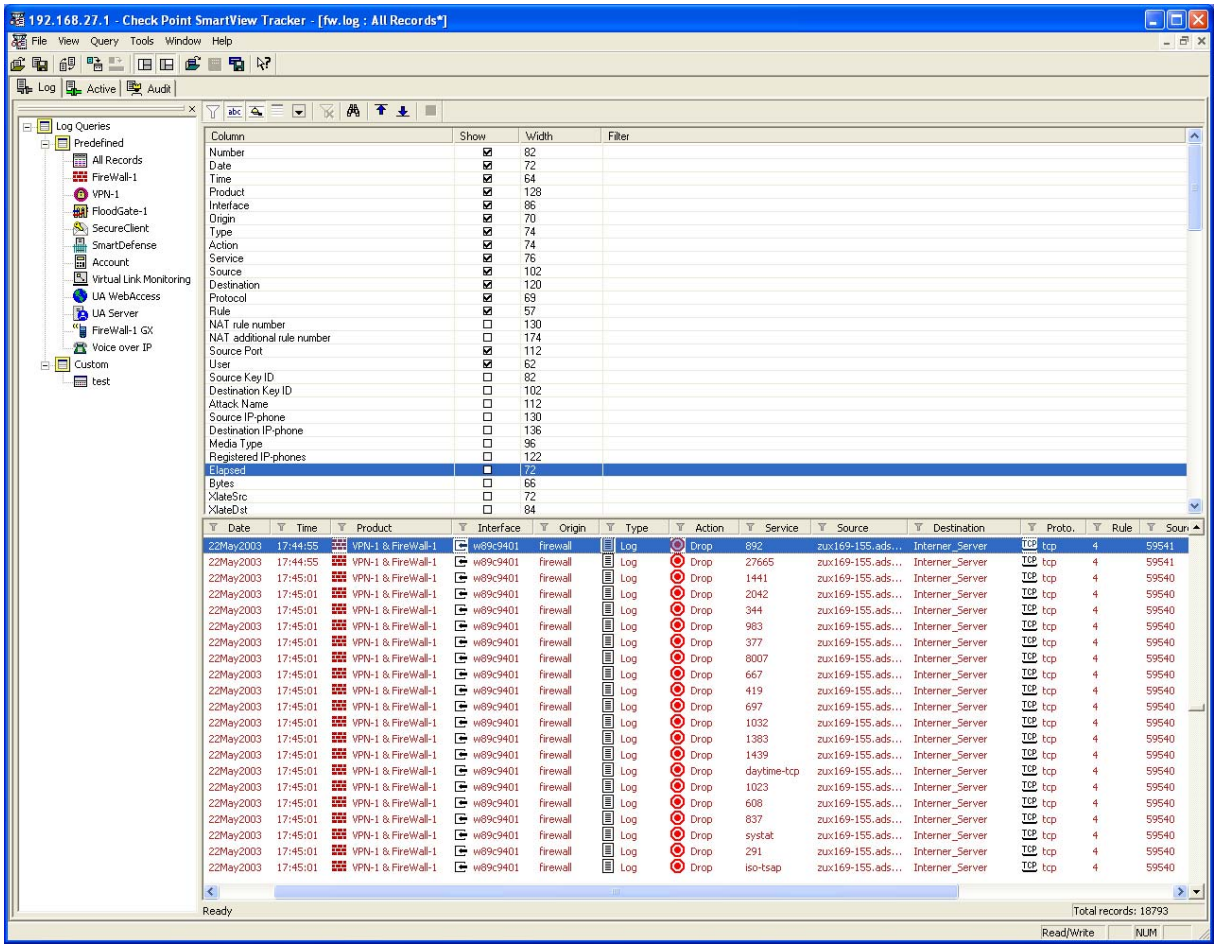

192.168.27.1 - Check Point SmartView Tracker - [fw.log : All Records*]
File View Query Tools Window Help
Log Active Audit
Log Queries
Predefined
All Records
FireWall-1
VPN-1
FloodGate-1
SecureClient
SmartDefense
Account
Virtual Link Monitoring
UA WebAccess
UA Server
FireWall-1 GX
Voice over IP
Custom
test
Column Show Width Filter
Number 82
Date 72
Time 64
Product 128
Interface 86
Origin 70
Type 74
Action 74
Service 76
Source 102
Destination 120
Protocol 69
Rule 57
NAT rule number 130
NAT additional rule number 174
Source Port 112
User 62
Source Key ID 82
Destination Key ID 102
Attack Name 112
Source IP-phone 130
Destination IP-phone 136
Media Type 96
Registered IP-phones 122
Elapsed 72
Bytes 66
XlateSrc 72
XlateDst 84
Date Time Product Interface Origin Type Action Service Source Destination Proto. Rule
22May2003 17:44:55 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 892 zux169-155.ads... Interner_Server tcp 4 59541
22May2003 17:44:55 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 27665 zux169-155.ads... Interner_Server tcp 4 59541
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 1441 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 2042 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 344 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 983 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 377 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 8007 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 667 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 419 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 697 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 1032 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 1383 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 1439 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop daytime-tcp zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 1023 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 608 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 837 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop systat zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop 291 zux169-155.ads... Interner_Server tcp 4 59540
22May2003 17:45:01 VPN-1 & FireWall-1 w89c9401 firewall Log Drop iso-tsap zux169-155.ads... Interner_Server tcp 4 59540
Ready
Total records: 18793
Read/Write
NUM

Abbildung 33: Check Point Firewall-1 NG – Bildschirmausgabe der Log-Dateieinträge

Neben der eigentlichen Log-Datei können über den „SmartView Tracker“ die zurzeit aktiven Verbindungen und Audit-Informationen (Angaben zu administrativen Logins auf der Firewall, zu Regel-Änderungen, zu Policy-Anpassungen, zur Erfassung neuer Objekte usw.) angezeigt werden.

Die Log-Einträge können jederzeit in einer Datei gespeichert und zu einem späteren Zeitpunkt auch problemlos im „SmartView Tracker“ wieder eingelesen und angezeigt werden.

Fazit Logging-Möglichkeiten und Alarmierung

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕ ⊖

- Die unmittelbare Alarmierung von Ereignissen kann auf die Systemkonsole, an eine E-Mail-Adresse, an einen System-Management-Server oder benutzerdefiniert erfolgen
- Die in der Log-Datei aufgezeichneten Daten sind

sehr umfassend und lassen sich beliebig auf dem Bildschirm ausgeben

- In den Log-Dateien kann effizient und effektiv gesucht werden. Auf die Einträge können beliebige und kumulativ wirksame Filter angewendet werden
- Die Log-Dateien lassen sich archivieren und zu einem späteren Zeitpunkt wiederum problemlos zur Bildschirmausgabe einlesen
- Systemrelevante Firewall-Aktivitäten wie der administrative Zugriff auf die Firewall, Änderungen von Firewall-Regeln und der Firewall-Policy werden in einem separaten Log festgehalten (Auditing)
- Sehr hohe Flexibilität sowohl bei den Alarmierungsmöglichkeiten als auch bei der Auswertung der geloggten Ereignisse

7.3.6 Network Address Translation (NAT)

Die Check Point Firewall-1 NG unterstützt, wie die beiden anderen getesteten Firewalls, dynamisches und statisches NAT:

NAT-Bezeichnung Check Point Firewall-1 NG	Typ	Interne IP-Adresse(n)	Externe IP-Adresse(n)
Dynamic (Hide) Mode NAT	dynamisch	192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 […]	80.254.159.30
Static Mode NAT	statisch	192.168.1.10 192.168.1.11 192.168.1.12	80.254.159.30 80.254.159.31 80.254.159.32

Tabelle 21: Check Point Firewall-1 NG – NAT-Konfigurationsmöglichkeiten

Die NAT-Regeln werden entweder durch die Firewall aufgrund der Einstellungen bei den einzelnen Objekten automatisch generiert (siehe Abbildung 34) oder können analog zu den Firewall Sicherheits-Policy-Regeln manuell konfiguriert werden.

Security - Standard | Address Translation - Standard | VPN Manager | Desktop Security - Standard

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	FTP_Server	* Any	* Any	FTP_Server (Valid Address)	= Original	= Original	* All	Automatic rule (see the network object data).
2	* Any	FTP_Server (Valid Address)	* Any	= Original	FTP_Server	= Original	* All	Automatic rule (see the network object data).
3	HOME-WS	* Any	* Any	HOME-WS (Valid Address)	= Original	= Original	* All	Automatic rule (see the network object data).
4	* Any	HOME-WS (Valid Address)	* Any	= Original	HOME-WS	= Original	* All	Automatic rule (see the network object data).
5	Internes_Netz	Internes_Netz	* Any	= Original	= Original	= Original	* All	Automatic rule (see the network object data).
6	Internes_Netz	* Any	* Any	Internes_Netz (Hiding Address)	= Original	= Original	* All	Automatic rule (see the network object data).

Abbildung 34: Check Point Firewall-1 NG – Automatisch generierte NAT-Regeln

Fazit NAT

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕ ⊖

- Die Firewall unterstützt sowohl dynamisches als auch statisches NAT
- Durch NAT sind die internen Systeme aus dem Internet nicht direkt ersichtlich

7.3.7 Virtual Private Network (VPN)

Der Firewall-Administrator kann bei der Check Point Firewall-1 NG FP3 zwischen verschiedenen VPN-Konfigurations-Methoden auswählen. Standardmässig wird die simplifizierte Methode verwendet. Bei dieser Methode werden die VPN-Policies von den Firewall-Policies getrennt und es müssen keine expliziten Verschlüsselungsregeln in der Firewall-Policy erfasst werden. Falls der Administrator die traditionelle VPN-Konfigurations-Methode, bei welcher die Verschlüsselungsregeln in der Firewall-Policy erfasst werden müssen, bevorzugt, kann er auf diese Methode zurückwechseln.

Das VPN basiert, wie bei den beiden anderen Firewalls, auf IPSec (Internet Protocol Security). Auch Check Point unterstützt sowohl das ESP-Protokoll mit den kryptographischen Algorithmen DES und 3DES und zusätzlich noch CAST, AES-128 und AES-256 für die Vertraulichkeit und HMAC-MD5 und HMAC-SHA-1 für die Authentizität der Daten als auch das AH-Protokoll mit den kryptographischen Algorithmen HMAC-MD5 und HMAC-SHA-1 für die Authentizität der Daten.

Das Schlüsselmanagement erfolgt über das IKE-Protokoll (Internet Key Exchange). Die Tests bezüglich VPN-Interoperabilität zwischen der Check Point Firewall-1 NG und der ZyWALL 10W (siehe auch Kapitel 5.3.9) und zwischen der Check Point Firewall-1 NG und der SonicWALL SOHO3 (siehe auch Kapitel 6.3.10) verliefen erfolgreich. Sowohl der VPN-Verbindungsaufbau zwischen der Check Point Firewall-1 NG und der ZyWALL 10W als auch zwischen der Check Point Firewall-1 NG und der SonicWALL SOHO3 klappte, sogar mit den höchsten Sicherheitseinstellungen, ohne Probleme (siehe Abbildung 35). Bis es soweit war,

mussten jedoch etliche Einstellungen auf der Check Point Firewall vorgenommen werden. Der ganze Vorgang erwies sich als relativ komplex und die Handbücher von Check Point konnten zur Fülle der Einstellungsmöglichkeiten nur bedingt Hilfe leisten. Dank der nun integrierten simplifizierten VPN-Konfigurationsmethode gestaltet sich die VPN-Konfiguration jedoch nun einfacher als bei früheren Check Point Firewall-Versionen. Die vorgenommenen VPN-Einstellungen und die zugrunde liegenden Konfigurationen der verschiedenen Firewalls sind im Anhang, in den Kapiteln 13.2.2, 13.2.3 und 13.2.4 ersichtlich.

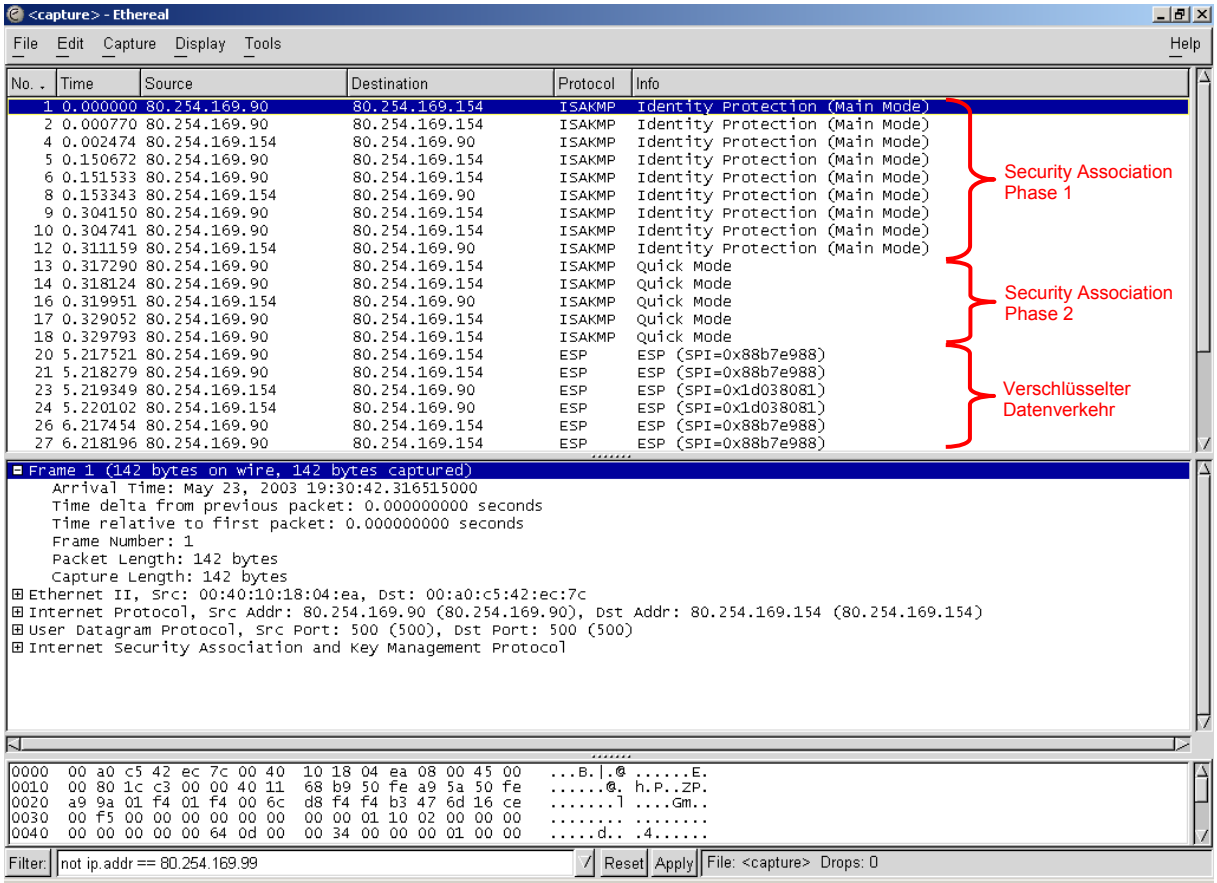

<capture> - Ethereal
File Edit Capture Display Tools Help
No. Time Source Destination Protocol Info
1 0.000000 80.254.169.90 80.254.169.154 ISAKMP Identity Protection (Main Mode)
2 0.000770 80.254.169.90 80.254.169.154 ISAKMP Identity Protection (Main Mode)
4 0.002474 80.254.169.154 80.254.169.90 ISAKMP Identity Protection (Main Mode)
5 0.150672 80.254.169.90 80.254.169.154 ISAKMP Identity Protection (Main Mode)
6 0.151533 80.254.169.90 80.254.169.154 ISAKMP Identity Protection (Main Mode)
8 0.153343 80.254.169.154 80.254.169.90 ISAKMP Identity Protection (Main Mode)
9 0.304150 80.254.169.90 80.254.169.154 ISAKMP Identity Protection (Main Mode)
10 0.304741 80.254.169.90 80.254.169.154 ISAKMP Identity Protection (Main Mode)
12 0.311159 80.254.169.154 80.254.169.90 ISAKMP Identity Protection (Main Mode)
13 0.317290 80.254.169.90 80.254.169.154 ISAKMP Quick Mode
14 0.318124 80.254.169.90 80.254.169.154 ISAKMP Quick Mode
16 0.319951 80.254.169.154 80.254.169.90 ISAKMP Quick Mode
17 0.329052 80.254.169.90 80.254.169.154 ISAKMP Quick Mode
18 0.329793 80.254.169.90 80.254.169.154 ISAKMP Quick Mode
20 5.217521 80.254.169.90 80.254.169.154 ESP ESP (SPI=0x88b7e988)
21 5.218279 80.254.169.90 80.254.169.154 ESP ESP (SPI=0x88b7e988)
23 5.219349 80.254.169.154 80.254.169.90 ESP ESP (SPI=0x1d038081)
24 5.220102 80.254.169.154 80.254.169.90 ESP ESP (SPI=0x1d038081)
26 6.217454 80.254.169.90 80.254.169.154 ESP ESP (SPI=0x88b7e988)
27 6.218196 80.254.169.90 80.254.169.154 ESP ESP (SPI=0x88b7e988)
Security Association Phase 1
Security Association Phase 2
Verschlüsselter Datenverkehr
Frame 1 (142 bytes on wire, 142 bytes captured)
Arrival Time: May 23, 2003 19:30:42.316515000
Time delta from previous packet: 0.000000000 seconds
Time relative to first packet: 0.000000000 seconds
Frame Number: 1
Packet Length: 142 bytes
Capture Length: 142 bytes
Ethernet II, Src: 00:40:10:18:04:ea, Dst: 00:a0:c5:42:ec:7c
Internet Protocol, Src Addr: 80.254.169.90 (80.254.169.90), Dst Addr: 80.254.169.154 (80.254.169.154)
User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
Internet Security Association and Key Management Protocol
0000 00 a0 c5 42 ec 7c 00 40 10 18 04 ea 08 00 45 00 ...B.|.@ ......E.
0010 00 80 1c c3 00 00 40 11 68 b9 50 fe a9 5a 50 fe ......@. h.P..ZP.
0020 a9 9a 01 f4 01 f4 00 6c d8 f4 f4 b3 47 6d 16 ce ....l ....Gm..
0030 00 f5 00 00 00 00 00 00 00 00 01 10 02 00 00 00 ....
0040 00 00 00 00 00 64 0d 00 00 34 00 00 00 01 00 00 .....d.. .4......
Filter: not ip.addr == 80.254.169.99 Reset Apply File: <capture> Drops: 0

Abbildung 35: Check Point Firewall-1 NG – Sniffer-Output des VPN-Verbindungsaufbaus mit der SonicWALL SOHO3

Um die Tests zwischen der Check Point Firewall-1 NG und der ZyWALL 10W bzw. der SonicWALL SOHO3 durchzuführen, wurde folgende Versuchsumgebung aufgebaut:

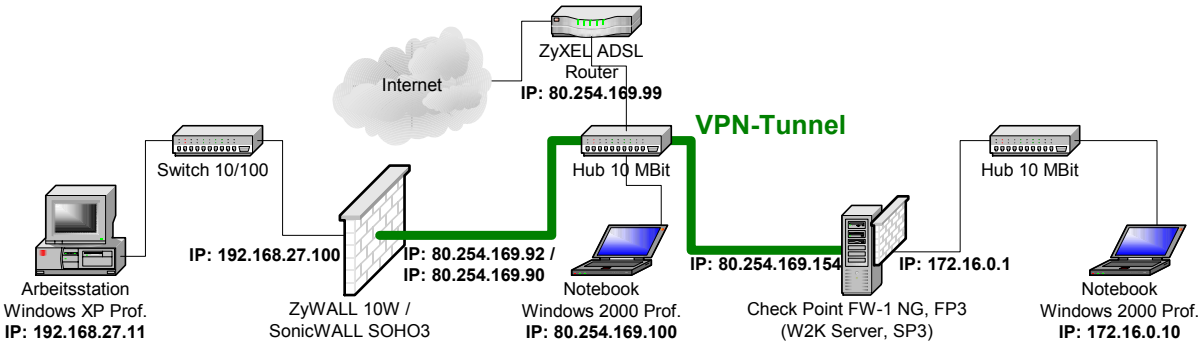


Abbildung 36: Check Point Firewall-1 NG – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der ZyWALL 10W bzw. der SonicWALL SOHO3

In der Log-Datei der Check Point Firewall kann aufgezeichnet werden, wie die Datenpakete bei einer VPN-Verbindung zwischen zwei End-Systemen (hier mit den IP-Adressen 192.168.27.11 und 172.16.0.10) auf der Check Point Firewall verschlüsselt (Action „Encrypt“) und entschlüsselt (Action „Decrypt“) werden:

N	Date	Time	Product	Interface	Origin	Type	Action	Service	Source	Destination	Pro...			Information
1	23May2003	16:00:21	VPN-1 & FireWall-1	daemon	80.254.169.154	Log	Key Install		80.254.169.90	80.254.169.154				IKE: Informational Exchange Rec
2	23May2003	16:00:21	VPN-1 & FireWall-1	daemon	80.254.169.154	Log	Key Install		80.254.169.90	80.254.169.154				IKE: Quick Mode completion; IKE
3	23May2003	16:00:32	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt		192.168.27.11	172.16.0.10	icmp	1		icmp-type: 8; icmp-code: 0;
4	23May2003	16:00:39	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Encrypt		172.16.0.10	192.168.27.11	icmp	1		icmp-type: 8; icmp-code: 0;
5	23May2003	16:01:04	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Encrypt	445	172.16.0.10	192.168.27.11	tcp	1	1...	
6	23May2003	16:01:04	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Encrypt	139	172.16.0.10	192.168.27.11	tcp	1	1...	
7	23May2003	16:01:04	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Drop	139	192.168.218.1	192.168.27.11	tcp		1...	message_info: Address spoofing;
8	23May2003	16:01:04	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Drop	139	192.168.241.1	192.168.27.11	tcp		1...	message_info: Address spoofing;
9	23May2003	16:01:04	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Drop		80.254.169.99	80.254.169.154	icmp			icmp-type: 5; icmp-code: 1; mess
10	23May2003	16:01:48	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Encrypt		172.16.0.10	192.168.27.11	icmp	1		icmp-type: 8; icmp-code: 0;
11	23May2003	16:02:07	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt		192.168.27.11	172.16.0.10	icmp	1		icmp-type: 8; icmp-code: 0;
12	23May2003	16:02:07	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Drop		80.254.169.99	80.254.169.154	icmp			icmp-type: 5; icmp-code: 1; mess
13	23May2003	16:02:37	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt	445	192.168.27.11	172.16.0.10	tcp	1	1...	
14	23May2003	16:02:37	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt	139	192.168.27.11	172.16.0.10	tcp	1	1...	
15	23May2003	16:02:42	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Accept	138	172.16.0.1	172.16.0.255	udp	1	138	encryption fail reason: Both endp
16	23May2003	16:02:42	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Accept	137	172.16.0.1	172.16.0.255	udp	1	137	encryption fail reason: Both endp
17	23May2003	16:02:57	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Drop	137	192.168.218.1	80.254.170.170	udp		137	message_info: Address spoofing;
18	23May2003	16:02:57	VPN-1 & FireWall-1	FA31x7	80.254.169.154	Log	Drop	137	192.168.241.1	80.254.170.170	udp		137	message_info: Address spoofing;
19	23May2003	16:02:58	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt	80	192.168.27.11	172.16.0.10	tcp	1	1...	
20	23May2003	16:02:58	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt	80	192.168.27.11	172.16.0.10	tcp	1	1...	
21	23May2003	16:02:58	VPN-1 & FireWall-1	w89c9401	80.254.169.154	Log	Decrypt	80	192.168.27.11	172.16.0.10	tcp	1	1...	

Abbildung 37: Check Point Firewall-1 NG – Log-Einträge einer VPN-Verbindung

Check Point bietet die zwei eigenen VPN-Clients SecuRemote Client und SecureClient an. Der Unterschied besteht unter anderem darin, dass der SecureClient neben der VPN-Client-Funktionalität auch noch eine Personal Firewall und weitere Schutzmechanismen beinhaltet, welche verhindern sollen, dass Dritte über das Internet mittels VPN-Client, wie in Abbildung 38[44] gezeigt, unbemerkt Zugriff auf das interne Netzwerk des Unternehmens erlangen.

[44] Quelle: Check Point Software Technologies Ltd., vgl. Check Point Desktop Security Guide NG FP2, Part No.: 700361, Nov. 2001, Seite 96

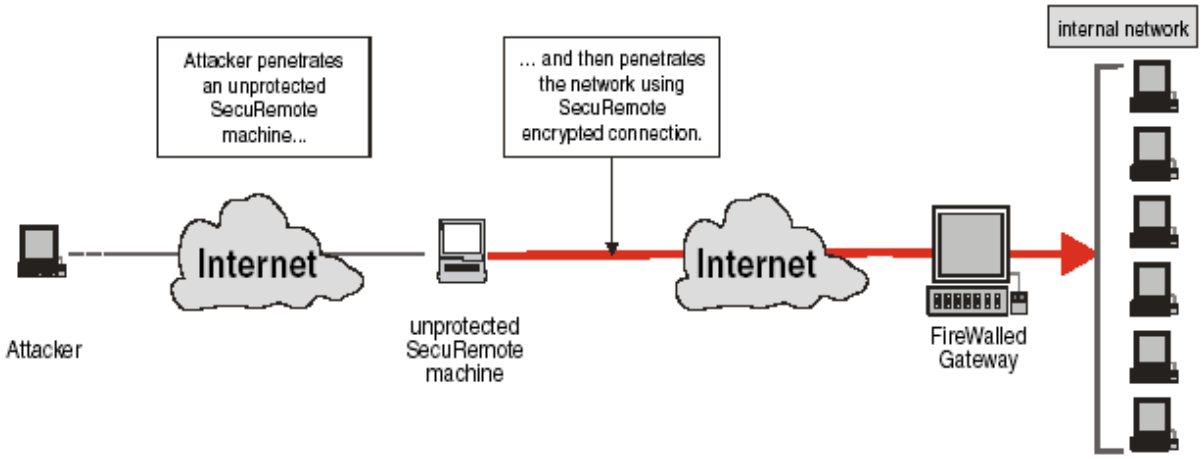


Abbildung 38: Check Point Firewall-1 NG – Unberechtigte Kontrolle über einen Arbeitsplatz mit SecuRemote

Damit die Benutzer mit den VPN-Clients Zugriff auf die Firewall resp. auf die sich dahinter befindenden internen Netzwerke oder Systeme nehmen können, müssen sie zuerst durch den Firewall-Administrator auf der Firewall als Benutzer erfasst werden. Die Authentisierung für den Zugriff kann mittels Benutzernamen und Passwort oder aber mittels digitalen Zertifikats erfolgen. Nach der erfolgreichen Authentisierung auf der Firewall, besteht eine VPN-gesicherte Verbindung zwischen dem VPN-Client und der Firewall. Falls auf der Firewall die entsprechenden Regeln vorhanden sind, kann der Benutzer nun auf Systeme aus dem internen Netzwerk zugreifen. Dabei werden direkt die internen privaten IP-Adressen verwendet, denn dem VPN-Client ist die Netzwerk-Infrastruktur hinter der Firewall bekannt.

Obschon Check Point über eigene VPN-Clients verfügt, wurde auch bei der Check Point Firewall-1 NG versucht, mittels Windows 2000 IPSec VPN-Client eine VPN-Verbindung zwischen einem Windows 2000 Notebook und der Firewall herzustellen. Auch diese Verbindung konnte erfolgreich hergestellt werden, wobei zwingend digitale Zertifikate eingesetzt werden mussten. Die Verwendung eines „Preshared Keys“ für die Verbindungsaufnahme wurde von der Check Point Firewall nicht akzeptiert. Die Anleitungen zur Konfiguration des IPSec-basierten VPN-Clients unter Windows 2000 und zu den benötigten Einstellungen auf der Check Point Firewall sind im Anhang in den Kapiteln 13.2.5 und 13.2.6 zu finden.

<u>Fazit VPN</u>

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Sichere (verschlüsselte) Netzwerkverbindungen mit anderen VPN-Gateways (z.B. anderen Firewalls) und zwischen VPN-Clients und Firewall möglich
- Interoperabilität mit anderen Firewalls
- Viele VPN-Einstellungsmöglichkeiten, dadurch hohe Flexibilität

⊖

- VPN-Konfiguration ziemlich komplex (aufgrund der vielen Einstellungsmöglichkeiten)
- Check Point Handbücher verbesserungswürdig

- Check Point bietet eigene VPN-Clients an, mit welchen auf eine einfache Art und Weise eine VPN-Verbindung mit einer Check Point Firewall hergestellt werden kann
- Als VPN-Client lässt sich auch Windows 2000 (oder höher) mit IPSec verwenden

7.3.8 Remote-Management

Das Remote-Management erfolgt bei der Check Point Firewall-1 NG grundsätzlich mittels den SmartClients. Dazu zählen insbesondere das SmartDashboard NG FP3, der SmartView Tracker NG FP3, der SmartView Status NG FP3, das SmartUpdate NG FP3, der SmartView Monitor NG FP3 und der User Monitor NG FP3.

Auf dem Management-Server (SmartCenter-Server) muss zuerst konfiguriert werden, welche Management-Stationen Zugriff auf die Firewall haben sollen (aufgrund ihrer IP-Adresse, ihres Systemnamens usw.). Der Zugriff wird dabei mittels Benutzernamen, Passwort und SSL-Verschlüsselung geschützt, d.h., dass dadurch auch der Benutzername und das Passwort der Administrators von der Management-Station zum Management-Server immer verschlüsselt übertragen wird und deshalb von allfälligen Snifferattacken im internen Netzwerk geschützt ist (Analysen mit einem Sniffer haben ergeben, dass der SmartClient-Verkehr zum Management-Server effektiv, wie in den Handbüchern beschrieben, mittels SSL verschlüsselt wird). Es können mehrere Administratoren erfasst werden, wobei für jeden Administrator eine individuelle Rechtevergabe möglich ist (nur Lese- oder Lese- und Schreibrechte auf einzelne Module ⇨ siehe Abbildung 39).

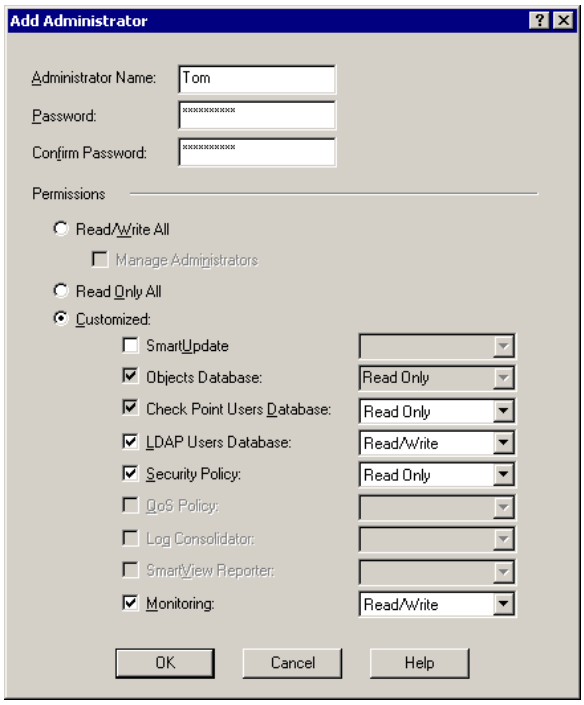


Abbildung 39: Check Point Firewall-1 NG – Zugriffsberechtigungen für Administratoren

Die Firewall-Regeln, welche für den Zugriff mit den SmartClients auf den Management-Server der Firewall nötig sind, werden durch die Firewall in den so genannten impliziten Firewall-Regeln (Implied Rules) automatisch definiert.

Generell setzt Check Point zum Schutz des Datenverkehrs zwischen allen Firewall-Modulen (inkl. Anbindung an OPSEC-Produkte von Dritten) ein so genanntes „Secure Internal Communications"-Verfahren ein. Dieses Verfahren basiert auf digitalen Zertifikaten (Check Point verfügt über eine eigene interne Certificate Authority) und SSL-Verschlüsselung. Auf diese Weise kann der Schutz der Vertraulichkeit und Authentizität der Kommunikation zwischen den Modulen gewährleistet werden.

Die Firewall beinhaltet zudem einen SNMP-Service, welcher auf den SNMP-Funktionalitäten der jeweils eingesetzten Betriebssysteme (Windows, Sun Solaris) beruht und als Ergänzung zu diesen dient. Auf diese Weise können Status-Informationen zur Firewall mittels Netzwerkmanagement-Tools (wie z.B. HP OpenView) abgefragt und überwacht werden. Standardmässig werden die Default-Community-Strings „public" und „private" verwendet; diese können jedoch beliebig angepasst werden.

Fazit Remote-Management

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Das Remote-Management erfolgt mit mehreren umfassenden Clients mit eigener grafischer Oberfläche
- Auf dem Management-Server kann definiert werden, welche Management-Stationen überhaupt auf den Server zugreifen dürfen
- Es können mehrere Administratoren mit unterschiedlichen Rechten erfasst werden
- Der Management-Datenverkehr wird verschlüsselt (inkl. Benutzernamen und Passwort des Administrators) und ist somit vor allfälligen Snifferattacken geschützt

⊖

7.3.9 Firewall-Updates

Check Point bietet ein „SmartUpdate"-Modul an, mit welchem die Check Point-Produkte zentral verwaltet und auf dem aktuellen Software-Stand gehalten werden können. Das „SmartUpdate"-Modul verlangt jedoch eine separate Lizenz, damit es eingesetzt werden kann.

Aber auch ohne den Einsatz des „SmartUpdate"-Moduls kann die Firewall-Software aktualisiert werden, wobei dieser Prozess im Unterschied zum SmartUpdate nicht automatisiert, sondern manuell erfolgt. Die Updates und Sicherheitspatches zu den einzelnen Modulen

können von der Check Point-Homepage[45] heruntergeladen und dann auf den entsprechenden Systemen installiert werden.

Fazit Firewall-Updates

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Hersteller führt Fehlerkorrekturen durch und stellt entsprechende Sicherheitspatches auf seiner Homepage zum Download zur Verfügung
- Download der aktuellen Softwareversionen von der Hersteller-Homepage problemlos möglich
- Optional kann ein zusätzliches Modul eingesetzt werden, welches die zentrale Verwaltung aller Check Point-Lizenzen im Netzwerk mit entsprechenden automatisierten Softwareupdates ermöglicht

⊖

7.3.10 Backup und Restore der Firewall-Konfiguration

Das Backup und Restore der Firewall (Management-Server resp. SmartCenter-Server) und allenfalls der einzelnen Module auf anderen Systemen (z.B. auf den Firewalled-Gateways) erfolgt grundsätzlich über die Backup- und Restore-Möglichkeiten der eingesetzten zugrunde liegenden Betriebssysteme. Falls lediglich ein Backup der Security-Policy (Regelwerk und Objekte der Firewall und die Benutzerdatenbank) erstellt werden soll, müssen folgende Dateien gesichert werden:

Backup von	***Zu sichernde Dateien***	***Dateiformat***
Firewall-Regelwerk	\$FWDIR/conf/*.W \$FWDIR/conf/rulebases_5_0.fws	ASCII
Firewall-Objekte	\$FWDIR/conf/objects_5_0.C	ASCII
Benutzerdatenbank	\$FWDIR/database/fwauth.NDB*	Binär

Tabelle 22: Check Point Firewall-1 NG – Backup der Firewall-Konfiguration

Der Platzhalter \$FWDIR steht für das Firewall-Verzeichnis. Unter Windows 2000 Server handelt es sich dabei normalerweise um das Verzeichnis " C:\WINNT\FW1\NG".

[45] Check Point-Homepage, siehe http://www.checkpoint.com

Fazit Backup und Restore der Firewall-Konfiguration

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕ ⊖

- Die Firewall-Konfiguration lässt sich durch das gezielte Kopieren einzelner Dateien sichern. Diese können bei Bedarf ohne Probleme wieder zurückgespielt werden, um die gesicherte Konfiguration wiederherzustellen

7.3.11 Hohe Verfügbarkeit und Load-Balancing

Zur Gewährung einer hohen Verfügbarkeit der Firewall-Infrastruktur und zum Einsatz von Load-Balancing (Check Point nennt diese Funktion „Load Sharing“) bietet Check Point ein eigenständiges Modul namens „Cluster XL“ an. Dieses muss separat lizenziert werden.

Im Bereich der hohen Verfügbarkeit ist vorgesehen, dass eine zweite identische Firewall im Netzwerk vorhanden ist, welche bei Ausfall der ersten Firewall deren Funktionalität übernimmt. Diese befindet sich im Hot-Standby-Modus (Leerlauf) und greift erst ins Geschehen ein, wenn die primäre Firewall ausfällt.

Beim Load-Balancing sind mehrere Firewalls parallel im Einsatz (so genannte Firewall-Clusters). Die Netzwerkverkehrslast wird dabei über alle Firewalls verteilt, womit sich die Gesamtleistung der Firewall-Infrastruktur erhöht. Mit Load-Balancing kann zudem gleichzeitig eine hohe Verfügbarkeit der Firewall-Infrastruktur erreicht werden, da bei Ausfall einer Firewall der Firewall-Cluster nach wie vor funktionstüchtig bleibt (lediglich die Gesamtleistung des Firewall-Clusters nimmt durch den Ausfall einer Firewall ab).

Sowohl beim Konzept der „hohen Verfügbarkeit“ als auch beim Load-Balancing führt Check Point eine so genannte „State Synchronization“ zwischen den Firewalls bzw. den Cluster-Mitgliedern durch. Der Status der aktiven Netzwerkverbindungen wird basierend auf dem „Stateful Inspection“-Konzept auf die Hot-Standby-Firewall oder auf die übrigen Cluster-Mitglieder synchronisiert. Falls nun eine Firewall ausfällt, können die während des Ausfalls aktiven Netzwerkverbindungen von der Hot-Standby-Firewall oder von den übrigen Cluster-Mitgliedern (praktisch) nahtlos übernommen und aufrecht erhalten werden.

Die Firewalls sind über ein so genanntes Synchronisationsnetzwerk miteinander verbunden; sie benötigen deshalb ein separates Interface, welches zu diesem Synchronisationsnetzwerk führt. Folgendes Netzwerkschema[46] zeigt diesen Sachverhalt auf:

[46] Quelle: Check Point Software Technologies Ltd., vgl. Check Point Firewall-1 Guide NG FP3, Part No.: 700527, September 2002, Seite 244

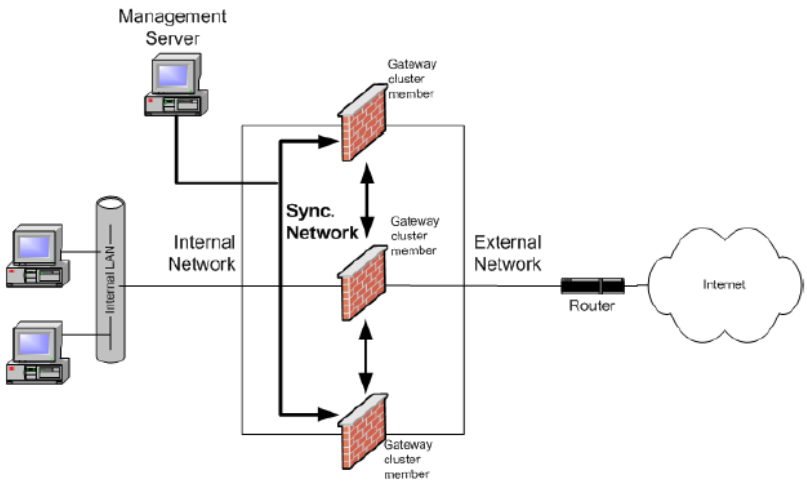


Abbildung 40: Check Point Firewall-1 NG – Netzwerkschema Firewall-Cluster

Check Point kennt noch eine weitere Form des Load-Balancing, wobei damit nicht die Netzwerklastverteilung auf die verschiedenen Firewalls innerhalb eines Firewall-Clusters gemeint ist, sondern die Netzwerklastverteilung auf verschiedene Server, welche sich hinter der Firewall befinden. Diese Funktion wird von Check Point „ConnectControl – Server Load Balancing" genannt. Der Netzwerkverkehr, welcher über die Firewall fliesst, kann dabei durch die Firewall auf verschiedene Server, welche alle den gleichen Dienst anbieten (z.B. Web-Server, FTP-Server usw.), verteilt werden. Die Gesamtleistung des angebotenen Dienstes (resp. der Server, welche den Dienst anbieten) kann auf diese Weise erhöht werden. Der Benutzer des Dienstes merkt jedoch nicht, dass mehrere Server im Einsatz sind (logisch gesehen handelt es sich um ein System, obschon physisch mehrere Server vorhanden sind).

<u>Fazit hohe Verfügbarkeit und Load-Balancing</u>

Beurteilung der Zusatzfunktionalität bezüglich Anwendbarkeit und/oder Nutzen ☺

Auswirkungen der Zusatzfunktionalität auf die Gesamtsicherheit der Firewall und/oder des LANs ☺

⊕

- Wie der Name bereits sagt, kann auf diese Weise die Verfügbarkeit der Firewall-Infrastruktur und letztlich des Netzwerkübergangs vom LAN ins WAN und umgekehrt hoch gehalten werden
- Check Point bietet neben der Möglichkeit, eine hohe Verfügbarkeit zu realisieren, ein Load-Balancing in einem Firewall-Cluster an. Damit wird die Last des Netzwerkverkehrs über mehrere Firewalls verteilt, was sich auch positiv auf die Verfügbarkeit auswirkt (kürzere Antwortzeiten)
- Die Statusinformationen der aktiven Netzwerkverbindungen werden auf die Hot-Standby-Firewall oder auf die anderen Firewalls im Cluster synchronisiert. Bei einem Ausfall einer Firewall gehen die bestehenden Netzwerkverbindungen nicht verloren und der Benutzer merkt im besten Fall nichts vom

⊖

Firewall-Ausfall

- Check Point hat nicht nur ein Load-Balancing für die Firewalls untereinander implementiert, sondern auch ein Load-Balancing für die Server (Web-Server, FTP-Server usw.) hinter der Firewall („ConnectControl – Server Load Balancing“)

8. GEGENÜBERSTELLUNG DER VERSCHIEDENEN ZUSATZFUNKTIONALITÄTEN

In diesem Kapitel werden die unter Kapitel 2 beschriebenen generischen Zusatzfunktionalitäten den analysierten Zusatzfunktionalitäten der drei untersuchten Firewalls gegenübergestellt. Dabei fliessen auch die durch den Autor vorgenommenen Bewertungen der Zusatzfunktionalitäten ein.

Wie aus der untenstehenden Tabelle ersichtlich ist, werden viele der untersuchten Zusatzfunktionalitäten den Erwartungen bezüglich ihrer Anwendbarkeit und ihres Nutzens mehrheitlich gerecht und nur wenige Zusatzfunktionalitäten beeinflussen die Gesamtsicherheit der Firewall oder der sich dahinter befindenden LANs negativ.

Die meisten der erwähnten Zusatzfunktionalitäten erachtet der Autor für die durch die Hersteller angesprochenen Zielgruppen als sinnvolle Ergänzung zur Grundfunktionalität einer Firewall. Einige der an und für sich interessanten und sinnvollen Ergänzungen weisen in ihrer Implementation jedoch gewisse Schwächen auf, was dazu führt, dass der Nutzen oder die Anwendbarkeit der Zusatzfunktionalität für den Firewall-Betreiber reduziert wird. Auf jeden Fall muss sich der Firewall-Betreiber der Grenzen der jeweiligen Zusatzfunktionalitäten seiner eingesetzten Firewall bewusst sein; nur auf diese Weise können das damit vorhandene „Restrisiko“ effektiv beurteilt und entsprechende Massnahmen getroffen werden.

Die in der Tabelle verwendete Symbolik (Erläuterungen dazu sind in Kapitel 1.5 zu finden) entspricht derjenigen, welche bei der Detailanalyse der einzelnen Zusatzfunktionalitäten verwendet wurde. Die Bewertung jeder untersuchten Zusatzfunktionalität eines jeden Produkts wird getrennt nach Anwendbarkeit/Nutzen und Einfluss auf die Sicherheit vorgenommen. Bei jeder Zusatzfunktionalität wurden Verweise auf die Kapitel, in welchen diese Zusatzfunktionalität erwähnt und analysiert wurde, angebracht.

Erklärung zu den Spaltenüberschriften der Übersichtstabelle:

Spaltenüberschrift	***Erklärung***
Zusatzfunktionalität	Bezeichnung der Zusatzfunktionalitäten, wie sie in Kapitel 2 erwähnt wurden
Sinnvoll – Ja/Nein	Erachtet der Autor die Implementation dieser Zusatzfunktionalität auf einer Firewall als sinnvoll oder nicht
Sinnvoll – Kap.	Referenz auf Kapitel, in welchem die Zusatzfunktionalität generisch umschrieben und bewertet wurde
Vorhand.	Ist die Zusatzfunktionalität auf der entsprechenden Firewall vorhanden? ⇨ Ja / Nein; Mittels Drittprodukt möglich (z.B. Anbindung mittels OPSEC-Schnittstelle); Auf Betriebssystemebene (OS-Ebene) implementiert bzw. vorhanden
Nutzen	Bewertung des Nutzens der Zusatzfunktionalität, so wie sie auf der entsprechenden Firewall implementiert wurde
Sicherheit	Bewertung der Sicherheit der Zusatzfunktionalität, so wie sie auf der entsprechenden Firewall implementiert wurde
Kap.	Referenz auf Kapitel, in welchem die Zusatzfunktionalität der entsprechenden Firewall analysiert und bewertet wurde

Zusatzfunktionalität	Sinnvoll		ZyXEL ZyWALL 10W				SonicWALL SOHO3				Check Point Firewall-1 NG FP3			
	Ja/Nein	Kap.	Vorhand.	Nutzen	Sicherheit	Kap.	Vorhand.	Nutzen	Sicherheit	Kap.	Vorhand.	Nutzen	Sicherheit	Kap.
Authentisierungsmöglich-keiten	Ja	2.1	Nein	-	-	-	Ja	☺	☺	6.3.1	Ja	☺	☺	7.3.1
Zeiteinschränkung einzelner Firewall-Regeln	Ja	2.2	Nein	-	-	-	Ja	☺	☺	6.3.2	Ja	☺	☺	7.3.2
URL-Filtering, URL-Blocking	Ja	2.3	Ja	😐	☺	5.3.1	Ja	😐	☺	6.3.3	Mittels Drittprod. möglich	-	-	-
Content-Filtering	Ja	2.4	Ja	😐	☺	5.3.1	Ja	😐	☺	6.3.3	Ja	☺	☺	7.3.3
Virenprüfung	Nein	2.5	Nein	-	-	-	Ja	☺	☺	6.3.4	Mittels Drittprod. möglich	-	-	-
SMTP-Filtering	Ja	2.6	Nein	-	-	-	Nein	-	-	-	Ja	☺	☺	7.3.3
Spam-Filtering	Nein	2.7	Nein	-	-	-	Nein	-	-	-	Mittels Drittprod. möglich	-	-	-
„Intrusion Detection"-Funktionen	Ja	2.8	Ja	😐	☺	5.3.2	Ja	☺	☺	6.3.5	Ja	☺	☺	7.3.4
Anti-Spoofing (IP-Spoofing)	Ja	2.9	Ja	☺	☺	5.3.2	Ja	☺	☺	6.3.5	Ja	☺	☺	7.3.4
Überwachung der Internetak-tivitäten	Ja	2.10	Nein	-	-	-	Ja	☺	☺	6.3.6	Mittels Drittprod. möglich	-	-	-
Erweiterte Logging-Möglichkeiten	Ja	2.11	Ja	😐	☺	5.3.3	Ja	😐	☺	6.3.6	Ja	☺	☺	7.3.5
Alarmierung	Ja	2.12	Ja	☺	☺	5.3.3	Ja	☺	☺	6.3.6	Ja	☺	☺	7.3.5
Unterstützung von NAT und/oder PAT	Ja	2.13	Ja	☺	-	5.3.4	Ja	☺	-	6.3.7	Ja	☺	☺	7.3.6
DHCP-Server	Ja	2.14	Ja	☺	-	5.3.5	Ja	☺	-	6.3.8	Auf OS-Ebene impl.	-	-	-

Zusatzfunktionalität	Sinnvoll		ZyXEL ZyWALL 10W				SonicWALL SOHO3				Check Point Firewall-1 NG FP3			
	Ja/Nein	Kap.	Vorhand.	Nutzen	Sicherheit	Kap.	Vorhand.	Nutzen	Sicherheit	Kap.	Vorhand.	Nutzen	Sicherheit	Kap.
Zeitserver-Dienst	Ja	2.15	Ja	☺	☺	5.3.6	Ja	☺	☺	6.3.9	Auf OS-Ebene impl.	-	-	-
Dynamisches DNS	Ja	2.16	Ja	☺	☹	5.3.7	Nein	-	-		Mittels Software auf OS-Ebene	-	-	-
Wireless-LAN (WLAN)	Nein	2.17	Ja	😐	☹	5.3.8	Nein	-	-		Nein	-	-	-
Virtual Private Network (VPN)	Ja	2.18	Ja	😐	☺	5.3.9	Ja	☺	☺	6.3.10	Ja	☺	☺	7.3.7
Diagnose-Tools	Ja	2.19	Ja	☺	-	5.3.10	Ja	☺	-	6.3.11	Auf OS-Ebene impl.	-	-	-
Remote-Management	Ja	2.20	Ja	☺	☹	5.3.11	Ja	☺	☺	6.3.12	Ja	☺	☺	7.3.8
Firmware- bzw. Firewall-Updates	Ja	2.21	Ja	☺	☺	5.3.12	Ja	☺	☺	6.3.13	Ja	☺	☺	7.3.9
Dial-Up-Backup, Verkehrsumleitung	Ja	2.22	Ja	☺	☺	5.3.13 5.3.14	Nein	-	-	-	Auf OS-Ebene impl.	-	-	-
Backup und Restore der Firewall-Konfiguration	Ja	2.23	Ja	☺	☺	5.3.15	Ja	☺	☺	6.3.14	Ja	☺	☺	7.3.10
Hohe Verfügbarkeit	Ja	2.24	Nein	-	-	-	Ja	☺	☺	6.3.15	Ja	☺	☺	7.3.11
Lastverteilung / Load Balancing	Ja	2.25	Nein	-	-	-	Nein	-	-	-	Ja	☺	☺	7.3.11

Tabelle 23: Gegenüberstellung der verschiedenen Zusatzfunktionalitäten und deren Bewertung

Es fällt auf, dass auf der Check Point Firewall-1 NG im Vergleich zu den beiden anderen Firewalls am wenigsten der analysierten Zusatzfunktionalitäten direkt auf der Firewall implementiert sind. Jedoch unterstützt sie eindeutig am meisten Drittprodukte, mit welchen die benötigten zusätzlichen Funktionalitäten abgedeckt werden können. Auf diese Weise lassen sich bei der Check Point Firewall praktisch alle der untersuchten Zusatzfunktionalitäten implementieren. Diejenigen Zusatzfunktionalitäten, welche direkt auf der Check Point Firewall implementiert sind, wussten jedoch zu gefallen. Sie funktionierten wie vorgesehen und es konnten keine inhärenten Risiken festgestellt werden.

Anders sieht die Sachlage bei der ZyWALL- und der SonicWALL-Firewall aus. Sie verfügen gegenüber der Check Point Firewall über mehr Zusatzfunktionalitäten, welche direkt auf der Firewall implementiert sind, lassen sich jedoch nur eingeschränkt erweitern und durch Drittprodukte ergänzen. Ausserdem besteht die Tendenz, bei diesen beiden Firewalls, welche primär auf den KMU-Markt abzielen, Zusatzfunktionalitäten zu implementieren, welche die Gesamtsicherheit der Firewall oder der sich dahinter befindenden Netzwerke gefährden können. Solche Zusatzfunktionalitäten werden sicher durch den einen oder anderen Betreiber einer solchen Firewall geschätzt, es besteht jedoch die Gefahr, dass sich der Betreiber der damit verbundenen Risiken nicht bewusst ist und durch die Aktivierung einer solchen Zusatzfunktionalität somit nicht gewollte Risiken eingegangen werden.

9. SCHLUSSBEMERKUNGEN / FAZIT

Alle der getesteten Firewalls bieten durchaus interessante Zusatzfunktionalitäten. Es wurde ersichtlich, dass die Zusatzfunktionalitäten dabei recht gut auf die durch die Hersteller anvisierte Zielgruppe abgestimmt sind. So sind Zusatzfunktionalitäten wie z.B. dynamisches DNS, Wireless-LAN usw. sicher eher für den Heimbenützer oder die kleineren Unternehmen von Interesse, wo hingegen Optionen wie hohe Verfügbarkeit oder Load-Balancing vielmehr grössere Unternehmen ansprechen.

Besonders erfreulich ist der Umstand, dass mit jeder der getesteten Firewalls eine sichere VPN-Verbindung zu den anderen Firewalls hergestellt werden konnte; handelt es sich dabei doch heutzutage um eine der wichtigsten Zusatzfunktionalitäten, welche die Firewalls anzubieten haben. Auch dass als VPN-Client ein Windows 2000 Professional Arbeitsplatz mit entsprechender IPSec-Konfiguration (ohne dass ein zusätzlicher VPN-Client installiert werden muss) eingesetzt werden kann, stellt schon fast eine „kleinere Sensation" dar; war doch bis vor kurzem die Standardisierung basierend auf IPSec noch nicht sehr weit fortgeschritten und die VPN-Interoperabilität zwischen den verschiedenen Produkten somit ein Glücksspiel.

Wie in der Diplomarbeit aufgezeigt wurde, können einige der Zusatzfunktionalitäten, je nachdem wie sie durch die Firewall-Administratoren implementiert werden, die Gesamtsicherheit der Firewall oder der internen Netzwerke hinter der Firewall gefährden. Es ist deshalb besonders wichtig, dass sich die Firewall-Administratoren der allfälligen Risiken, die sie bei der Aktivierung solcher Zusatzfunktionalitäten eingehen, bewusst sind.

Ausserdem lassen sich manche der Zusatzfunktionalitäten, welche die Gesamtsicherheit der Firewall und der internen Netzwerke grundsätzlich verbessern, gezielt durch die Benutzer umgehen oder in ihrer Wirksamkeit reduzieren (z.B. beim Content- und URL-Filtering). Auch hier ist es wichtig, dass sich die IT-Verantwortlichen und die Firewall-Administratoren dieser Möglichkeiten bewusst sind, um entsprechende (Gegen-)Massnahmen, zum Teil auch organisatorischer Natur, ergreifen zu können.

Die vorliegende Diplomarbeit vermag sicher die sowohl positiven als auch negativen Eigenschaften einiger der heute vorhandenen und denkbaren Firewall-Zusatzfunktionalitäten anhand von konkreten Produkten aufzuzeigen und IT-Verantwortliche und Firewall-Administratoren bezüglich der damit allenfalls vorhandenen Risiken zu sensibilisieren. Zudem stellen die konkreten Konfigurationsanleitungen im Anhang der Arbeit eine nützliche Ergänzung dar, da sie Lösungen für komplexere Konfigurationssituationen (insbesondere im VPN-Umfeld) Schritt für Schritt aufzeigen und dadurch eigene mühsame und langwierige Abklärungen und Konfigurationstests vermieden werden können – der Autor spricht hier aus eigener Erfahrung ;-).

10. QUELLENVERZEICHNIS

10.1 Literaturverzeichnis

Check Point Software Technologies Ltd.: Check Point Getting Started Guide NG FP3, Part No.: 700510, Israel 2002

Check Point Software Technologies Ltd.: Check Point Firewall-1 Guide NG FP3, Part No.: 700527, Israel 2002

Check Point Software Technologies Ltd.: Check Point SmartCenter Guide NG FP3, Part No.: 700526, Israel 2002

Check Point Software Technologies Ltd.: Check Point Virtual Private Networks Guide NG FP3, Part No.: 700528, Israel 2002

Check Point Software Technologies Ltd.: Check Point Desktop Security Guide NG FP2, Part No.: 700361, Israel 2001

Hyams, David: Firewall Lösungen, Skript Nachdiplomstudium NDS-INS 4, Fachhochschule Zentralschweiz, Institut für Wirtschaftsinformatik Luzern 2003

Microsoft Press: Computer Lexikon / Fachwörterbuch, deutsch-englisch / englisch-deutsch, Unterschleissheim 2002

Pohlmann, Norbert: Firewall-Systeme, 4. Auflage, MITP-Verlag GmbH, Bonn 2001

SonicWALL, Inc.: SonicWALL – Internet Security Appliance, Rev. A 10/01, United States 2002

Zwicky, Elizabeth D.: Cooper, Simon: Chapman, D. Brent: Building Internet Firewalls, 2nd Edition, O'Reilly, United States 2000

ZyXEL Communications Corporation: ZyWALL 10/10W/50/100 – User's Guide, Version 3.52 and 3.60, Taiwan 2002

10.2 Verzeichnis von Internetadressen

Bezeichnung und Internet-Adresse:	***Datum:***
➢ Amazon – Homepage (Verwendung zu Testzwecken)	
`http://www.amazon.de`	07.05.03
➢ Anonymer Web-Proxy – Homepage	
`http://www.guardster.com`	07.05.03
➢ Check Point – Homepage	
`http://www.checkpoint.com`	25.05.03
➢ Common Criteria – Homepage des gleichnamigen Standards	
`http://www.commoncriteria.org`	21.04.03
➢ Cyber Patrol (URL-Filtering-Softwarehersteller) – Homepage	
`http://www.cyberpatrol.com`	07.05.03
➢ Dynamic-DNS – Liste von Anbietern:	
`http://www.technopagan.org/dynamic`	22.04.03
➢ Free Proxy Public Servers List – Homepage	
`http://tools.rosinstrument.com/proxy`	07.05.03
➢ Google-Suchmaschine – Homepage	
`http://www.google.com`	15.05.03
➢ Heise Browsercheck – Homepage	
`http://www.heise.de/ct/browsercheck/`	07.05.03
➢ ICSA Labs – Homepage einer Firewall-Zertifizierungsstelle:	
`http://www.icsalabs.com`	21.04.03
➢ JAP Anonymity & Privacy (lokaler Web-Proxy) – Homepage	
`http://anon.inf.tu-dresden.de/`	15.05.03

Bezeichnung und Internet-Adresse: ***Datum:***

- Liste von freien öffentlichen Proxy-Servern

`http://tools.rosinstrument.com/proxy/` 07.05.03

- Odyssey 802.1x-Client für Windows – Homepage

`http://www.funk.com/radius/wlan/wlan_c_radius.asp` 04.05.03

- Sicherheitsportal eSecurityOnline – Homepage (Verwendung zu Testzwecken)

`http://www.esecurityonline.com` 07.05.03

- SonicWALL Firewalls – Homepage Produktübersicht

`http://www.sonicwall.com/products/vpnapp.html` 07.05.03

- Swiss – Homepage (Verwendung zu Testzwecken)

`http://www.swiss.com/net/index/tg-ob-mp-create-and-change.htm` 07.05.03

- Thawte – Homepage einen Anbieters von digitalen Zertifikaten

`http://www.thawte.com` 07.05.03

- Tomsplace – Homepage des Autors (Verwendung zu Testzwecken)

`http://www.tomsplace.ch` 07.05.03

- Web Page Backward Compatibility Viewer – Homepage

`http://www.delorie.com/web/wpbcv.html` 15.05.03

- Websense Inc. – Hersteller von Filtering-Software – Homepage

`http://www.websense.com` 15.05.03

- Windows 2000 Patch: Using 802.1x Authentication on Computers Running Windows 2000

`http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6B78EDBE-D3CA-4880-929F-453C695B9637` 04.05.03

Bezeichnung und Internet-Adresse: ***Datum:***

- WorkGroup Solutions – Hersteller von Filtering-Software – Homepage

`http://www.n2h2filter.com` 15.05.03

- ZyXEL Firewalls – Homepage Produktübersicht

`http://www.zyxel.com/product/category.php?indexFlagvalue=1021873683` 07.05.03

11. VERZEICHNIS DER ABBILDUNGEN UND TABELLEN

11.1 Abbildungsverzeichnis

Abbildung 1: ZyWALL 10W – Versuchsumgebung für die Durchführung der Firewall-Tests 23
Abbildung 2: ZyWALL 10W URL-Filtering – manuelle Ergänzung der Filter-Liste 31
Abbildung 3: ZyWALL 10W – Durch die Firewall gemeldete vermeintliche Attacken beim Zugriff auf das Internet 34
Abbildung 4: ZyWALL 10W – Konfiguration der Attacken-Schwellenwerte 35
Abbildung 5: ZyWALL 10W – Erkennung von IP-Spoofing-Angriffen 36
Abbildung 6: ZyWALL 10W mit öffentlicher WAN-IP-Adresse für dynamisches DNS 41
Abbildung 7: ZyWALL 10W mit privater WAN-IP-Adresse (dynamisches DNS nur eingeschränkt möglich) 42
Abbildung 8: ZyWALL 10W – Wireless-Sicherheitslevels 44
Abbildung 9: ZyWALL 10W – VPN-Grundeinstellungen 45
Abbildung 10: ZyWALL 10W – Einstellungen IKE Schlüsselaushandlung 46
Abbildung 11: ZyWALL 10W – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der SonicWALL SOHO3 47
Abbildung 12: ZyWALL 10W – Sniffer-Output des verschlüsselten Datenverkehrs zwischen der ZyWALL 10W und der SonicWALL SOHO3 47
Abbildung 13: ZyWALL 10W – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der Check Point Firewall-1 NG 48
Abbildung 14: SonicWALL SOHO3 – Versuchsumgebung für die Durchführung der Firewall-Tests 55
Abbildung 15: SonicWALL SOHO3 – Zeiteinschränkung der Firewall-Regeln 59
Abbildung 16: SonicWALL SOHO3 – Aufforderung zur Installation des Anti-Virenprogramms 66
Abbildung 17: SonicWALL SOHO3 – Log-Einträge gefilterter Attachments 67
Abbildung 18: SonicWALL SOHO3 – Durch die Firewall korrekt erkannte Attacken 69
Abbildung 19: SonicWALL SOHO3 – Erkennung von Trojaner-Zugriffsversuchen 70
Abbildung 20: SonicWALL SOHO3 – Zeitabgleich mit Zeitserver 74
Abbildung 21: SonicWALL SOHO3 – VPN-Grundeinstellungen 75
Abbildung 22: SonicWALL SOHO3 – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der ZyWALL 10W 76
Abbildung 23: SonicWALL SOHO3 – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der Check Point Firewall-1 NG 76
Abbildung 24: Check Point Firewall-1 NG – Versuchsumgebung für die Durchführung der Firewall-Tests 84
Abbildung 25: Check Point Firewall-1 NG – Auswahl des Authentisierungstyps pro Firewall-Regel 87
Abbildung 26: Check Point Firewall-1 NG – Unverschlüsselte Session-Authentisierung 88
Abbildung 27: Check Point Firewall-1 NG – Mit SSL verschlüsselte Session-Authentisierung 88
Abbildung 28: Check Point Firewall-1 NG – Content-Filtering beim FTP-Dienst 90
Abbildung 29: Check Point Firewall-1 NG – SMTP-Filtering aufgrund des Attachment-Typs 91
Abbildung 30: Check Point Firewall-1 NG – SmartDefense-Einstellungsmöglichkeiten 93

Abbildung 31: Check Point Firewall-1 NG – Erkennung und Alarmierung von IP-Spoofing 94
Abbildung 32: Check Point Firewall-1 NG – Blocken von Paketen aufgrund ihrer TCP-Flags....94
Abbildung 33: Check Point Firewall-1 NG – Bildschirmausgabe der Log-Dateieinträge 96
Abbildung 34: Check Point Firewall-1 NG – Automatisch generierte NAT-Regeln 98
Abbildung 35: Check Point Firewall-1 NG – Sniffer-Output des VPN-Verbindungsaufbaus mit der SonicWALL SOHO3 99
Abbildung 36: Check Point Firewall-1 NG – Versuchsumgebung für die Durchführung der VPN-Interoperabilitätstests mit der ZyWALL 10W bzw. der SonicWALL SOHO3 100
Abbildung 37: Check Point Firewall-1 NG – Log-Einträge einer VPN-Verbindung....100
Abbildung 38: Check Point Firewall-1 NG – Unberechtigte Kontrolle über einen Arbeitsplatz mit SecuRemote 101
Abbildung 39: Check Point Firewall-1 NG – Zugriffsberechtigungen für Administratoren 102
Abbildung 40: Check Point Firewall-1 NG – Netzwerkschema Firewall-Cluster....106
Abbildung 41: ZyWALL 10W – Herunterladen der versteckten Datei "spt.dat" I
Abbildung 42: ZyWALL 10W – Inhalt der Datei "spt.dat" mit Hex-Editor angezeigt II
Abbildung 43: DynDNS – Kontozugriff mit SSL-Verschlüsselung III
Abbildung 44: DynDNS – Sniffer-Output der Anmeldeinformationen mit Base64-codiertem Passwort IV
Abbildung 45: DynDNS – Decodieren des Base64-codierten Passworts....IV
Abbildung 46: ZyWALL 10W – Übermittelter Benutzername für das URL-Filtering-Update V
Abbildung 47: ZyWALL 10W – URL-Filter-Datei V
Abbildung 48: ZyWALL 10W – Inhalt des URL-Filter-Update-Verzeichnisses VI
Abbildung 49: ZyWALL 10W – Inhalt der URL-Filter-Liste VII
Abbildung 50: ZyWALL 10W – Zugriff auf die Datei "/etc/passwd" des FTP-Servers VIII
Abbildung 51: ZyXEL Prestige 642R – Menu 1 (General Setup) IX
Abbildung 52: ZyXEL Prestige 642R – Menu 4 (Internet Access Setup) IX
Abbildung 53: ZyXEL Prestige 642R – Menu 11.1 (Remote Node Profile) X
Abbildung 54: ZyWALL 10W – VPN-Grundeinstellungen für VPN-Verbindung mit der SonicWALL SOHO3 XI
Abbildung 55: ZyWALL 10W – Erweitere VPN-Einstellungen für VPN-Verbindung mit der SonicWALL SOHO3 XI
Abbildung 56: ZyWALL 10W – VPN-Grundeinstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG XII
Abbildung 57: ZyWALL 10W – Erweitere VPN-Einstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG XII
Abbildung 58: SonicWALL SOHO3 – VPN-Grundeinstellungen für VPN-Verbindung mit der ZyWALL 10W XIII
Abbildung 59: SonicWALL SOHO3 – Erweitere VPN-Einstellungen für VPN-Verbindung mit der ZyWALL 10W XIII
Abbildung 60: SonicWALL SOHO3 – VPN-Grundeinstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG XIV
Abbildung 61: SonicWALL SOHO3 – Erweitere VPN-Einstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG....XIV
Abbildung 62: Versuchsumgebung für die Durchführung des VPN-Client-Tests XIX
Abbildung 63: ZyWALL 10W – VPN-Grundeinstellungen für Windows 2000 IPSec-Client XIX

Abbildung 64: ZyWALL 10W – Erweiterte VPN-Einstellungen für Windows 2000 IPSec-Client XX
Abbildung 65: SonicWALL SOHO3 – VPN-Einstellungen für Windows 2000 IPSec-Client XX

11.2 Tabellenverzeichnis

Tabelle 1: Verwendete Symbole zur Beurteilung, ob eine Zusatzfunktionalität sinnvoll erscheint 8
Tabelle 2: Verwendete Symbole beim Fazit zu den einzelnen Zusatzfunktionalitäten 8
Tabelle 3: Verwendete Symbole bei den Teilresultaten von Zusatzfunktionalitäten-Tests 9
Tabelle 4: ZyWALL 10W – Eigenschaften 21
Tabelle 5: SonicWALL SOHO3 – Eigenschaften 22
Tabelle 6: Check Point Firewall-1 NG – Eigenschaften 22
Tabelle 7: ZyWALL 10W Content-Filtering – durchgeführte Tests und Ergebnisse 28
Tabelle 8: ZyWALL 10W – Filter-Kategorien für das URL-Filtering 28
Tabelle 9: ZyWALL 10W URL-Filtering – durchgeführte Tests und Ergebnisse 31
Tabelle 10: ZyWALL 10W "Intrusion Detection" – Resultate diverser Portscans auf die Firewall 36
Tabelle 11: ZyWALL 10W – Logging-Kategorien 38
Tabelle 12: ZyWALL 10W – NAT-Konfigurationsmöglichkeiten 39
Tabelle 13: ZyWALL 10W – Resultate Portscans mit Firewall-Stealth-Modus 50
Tabelle 14: SonicWALL SOHO3 Content-Filtering – durchgeführte Tests und Ergebnisse 61
Tabelle 15: SonicWALL SOHO3 – Filter-Kategorien für das URL-Filtering 62
Tabelle 16: SonicWALL SOHO3 URL-Filtering – durchgeführte Tests und Ergebnisse 64
Tabelle 17: SonicWALL SOHO3 – Logging-Kategorien 71
Tabelle 18: SonicWALL SOHO3 – NAT-Konfigurationsmöglichkeiten 72
Tabelle 19: SonicWALL SOHO3 – Resultate Portscans mit Firewall-Stealth-Modus 80
Tabelle 20: Check Point Firewall-1 NG – Eigenschaften der Security Server 90
Tabelle 21: Check Point Firewall-1 NG – NAT-Konfigurationsmöglichkeiten 97
Tabelle 22: Check Point Firewall-1 NG – Backup der Firewall-Konfiguration 104
Tabelle 23: Gegenüberstellung der verschiedenen Zusatzfunktionalitäten und deren Bewertung 110

12. GLOSSAR

ADSL

Abkürzung für **A**symmetric **D**igital **S**ubscriber **L**ine. Technologie und Hardwarekomponenten, die Hochgeschwindigkeitsübertragungen von digitalen Signalen, Videosignale inbegriffen, über ein gewöhnliches, verdrilltes Kupfertelefonkabel erlaubt. Die Übertragungsgeschwindigkeit beim Empfang der Daten ist höher als beim Senden der Daten (aus Kundensicht).

Base64

Die Base64-Kodierung stellt ein einfaches Verfahren dar, um beliebige Daten in eine textorientierte Form zu bringen und sie auf diese Weise über ein Netzwerk zu übermitteln. Die Kodierung basiert auf 64 Zeichen (A-Z, a-z, 0-9, +, /), deshalb auch der Name Base64. Im RFC 2045 (Request for Comments) wird dieses Verfahren beschrieben.

CA

Abkürzung für **C**ertificate **A**uthority. Eine Organisation, die digitale Zertifikate herausgibt. Als CA kann sowohl eine spezialisierte externe Firma (z.B. VeriSign) oder eine Institution innerhalb einer Firma auftreten. Die Aufgabe einer CA ist, digitale Zertifikate herauszugeben und zu überprüfen. Sie ist dabei für die Bereitstellung und Zuweisung eindeutiger „Schlüssel" verantwortlich, die in digitalen Zertifikaten zur Authentifizierung sowie zur Verschlüsselung und Entschlüsselung sensitiver oder vertraulicher Daten dienen, welche über das Internet und andere Netze verbreitet werden.

DMZ

Abkürzung für **De**m**i**litarisierte **Z**one. Bezeichnet einen Computer bzw. ein kleines Netzwerk, das über eine Firewall zwischen das private Netzwerk eines Unternehmens und das öffentliche Netzwerk (Internet) geschaltet wird. Normalerweise soll Aussenstehenden auf die Systeme der DMZ ein eingeschränkter Zugriff gewährt werden (z.B. auf einen Web-Server). Es soll jedoch verhindert werden, dass Aussenstehende direkten Zugriff auf Daten im internen Netzwerk erhalten.

DoS-Attacke

Abkürzung für **D**enial **o**f **S**ervice-Attacke. Ein meist geplanter Versuch, ein System in der Verrichtung seiner normalen Tätigkeit zu stören. Eine DoS-Attacke überschüttet so z.B. einen Server mit Verbindungsanforderungen, die nicht ausgeführt werden können. Der Server ist dann mit der Reaktion auf die Attacke dermassen überlastet, dass er legitime Verbindungsanforderungen ignoriert. Andere Formen von DoS-Attacken beinhalten die Zerstörung oder Veränderung von Konfigurationsdaten des Servers, den unberechtigten Zugang zu physikalischen Komponenten des Systems usw. Eine DoS-Attacke kann ein Herunterfahren oder Einfrieren des angegriffenen Systems verursachen.

IKE

Abkürzung für **I**nternet **K**ey **E**xchange. Bei IKE handelt es sich um ein IPSec-Standardprotokoll, welches zur Sicherstellung von

	Sicherheit beim Schlüsselaustausch im Rahmen von VPNs verwendet wird. Es wird für die Security Association (SA) bei der Verbindungsinitialisierung von VPNs eingesetzt. Obschon IKE für den Einsatz von IPSec nicht zwingend gebraucht wird, bietet es einige Vorteile wie: automatische Schlüsselaushandlung und Authentisierung, Certificate Authority (CA) Unterstützung und die Möglichkeit, während einer IPSec-Session die Verschlüsselungs-Schlüssel auszutauschen.
IP Spoofing	Das Einfügen einer falschen IP-Absenderadresse in eine Datenübertragung. Das Ziel dieser Aktion ist der unberechtigte Zugriff auf ein Computersystem.
IPSec	Abkürzung für **I**nternet **P**rotocol **Sec**urity. Eine Gruppe aus Sicherheitsprotokollen, ESP („Encapsulating Security Payload“) und AH („Authentication Header“), die erhöhte Sicherheit, eine Integritätsprüfung, eine Authentifizierung und den Wiedergabeschutz bei Daten gewährleisten, die über die IP-Komponente (Internet Protocol) von TCP/IP im Internet übertragen werden. IPSec findet beispielsweise bei der Implementation von virtuellen privaten Netzwerken (VPNs) Anwendung.
ISP	Abkürzung für **I**nternet **S**ervice **P**rovider. Ein Unternehmen, das allgemeine Internet-Dienstleistungen an Privatpersonen, Unternehmen und andere Organisationen verkauft. Einige ISPs sind große nationale oder multinationale Unternehmen, die Internetzugriffe an verschiedenen Standorten anbieten. Es gibt auch lokale ISPs, die ihre Dienste nur in bestimmten Städten oder Bereichen zur Verfügung stellen.
L2TP	Abkürzung für **L**ayer **2** **T**unneling **P**rotocol. Ein Standard der Internet Engineering Task Force (IETF), der in RFC 2661 (Request for Comments) das Erstellen von VPNs (Virtuelle Private Netzwerke) über das Internet definiert. L2TP unterstützt mehrere Protokolle, wozu auch nicht auf IP basierende Protokolle (beispielsweise Appletalk and IPX) gehören. L2TP stellt eine Kombination der besten Funktionen von PPTP (Point-to-Point Tunneling Protocol, definiert in RFC 2637) und L2F (Cisco Layer 2 Forwarding, definiert in RFC 2341) dar.
LAN	Abkürzung für **L**ocal **A**rea **N**etwork. Ein lokales Netzwerk, das aus einer Gruppe von Computern und anderen Geräten besteht, die über einen relativ begrenzten Bereich verteilt und durch Kommunikationsleitungen verbunden sind, die jedem Gerät die Interaktion mit jedem anderen Gerät im Netzwerk ermöglichen. LANs bestehen häufig aus Mikrocomputern und gemeinsam genutzten Ressourcen, z.B. Laserdruckern und großen Festplatten. Die an einem LAN angeschlossenen Geräte bezeichnet man als Knoten. Die Verkabelung der Knoten untereinander stellt die Übertragung der Nachrichten sicher.
Land	Name einer DoS-Attacke. Durch die Land-Attacke wird ein sehr komplexer Angriff ausgeführt, welcher ein SYN-Paket mit identi-

	scher Absender- und Empfängeradresse des anzugreifenden Systems erzeugt. Für das angegriffene System sieht es dann so aus, als ob es sich das Paket selber gesendet hätte, was zu empfindlichen Störungen des Systems führen kann.
NAT	Abkürzung für **N**etwork **A**ddress **T**ranslation. Das Umwandeln von privaten IP-Adressen, die in einem Intranet oder anderen, privaten Netzwerk verwendet werden zu öffentlichen Internet IP-Adressen. Diese Methode ermöglicht die Verwendung einer grossen Anzahl von privaten IP-Adressen innerhalb des eigenen Netzwerkes, ohne die eingeschränkte Anzahl der verfügbaren öffentlichen IP-Adressen zu erschöpfen.
NetBIOS	Eine Anwendungsprogrammierschnittstelle (Application Programming Interface, API) für Anwendungsprogramme, die unter MS-DOS, OS/2 oder bestimmten UNIX-Versionen in einem lokalen Netzwerk aus IBM und kompatiblen Mikrocomputern laufen. NetBIOS ist hauptsächlich für Programmierer von Bedeutung und bietet Anwendungsprogrammen einen einheitlichen Befehlssatz für die Anforderung niederer Netzwerkdienste, die für die Durchführung von Sitzungen zwischen Knoten auf einem Netzwerk und den Informationsaustausch erforderlich sind.
OPSEC	Abkürzung für **O**pen **P**latform for **Sec**urity. Dabei handelt es sich um ein Allianzprogramm für Sicherheitsapplikationen und Sicherheitssystementwickler, welches 1997 durch Check Point erstellt wurde. Dieses Allianzprogramm stellt ein offenes industrieweites Rahmenmodell zur Gewährung der Interoperabilität von Sicherheitslösungen verschiedener Hersteller dar.
Ping of Death	Name einer DoS-Attacke. Dabei wird ein IP-Paket erzeugt, welches die maximal vorgesehene Byte-Grösse gemäss IP-Spezifikation überschreitet. Dieses übergrosse IP-Paket wird danach dem anzugreifenden System gesendet. Das angegriffene System stürzt dabei unter Umständen ab oder führt einen Neustart durch.
Portscan	Eine über das Netzwerk durchgeführte Überprüfung, welche Ports bzw. Dienste ein System anbietet. Ein Portscan wird oft als vorbereitende Handlung für einen möglichen Systemangriff durchgeführt (Auskundschaften des anzugreifenden Systems).
PPP	Abkürzung für **P**oint-to-**P**oint **P**rotocol. Ein Datenverbindungsprotokoll der Internet Engineering Task Force, das 1991 für Wählverbindungen (z.B. zwischen einem Computer und einem Internet-Provider) vorgestellt wurde.
PPPoE	Abkürzung für **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. Dabei handelt es sich um eine Spezifikation, um mehrere Computerbenutzer eines LAN an einen entfernten Standort (z.B. Internet Provider) anzubinden (z.B. mittels Modem oder ähnlichen Geräten). PPPoE kombiniert das PPP-Protokoll (häufig in Wählverbindun-

	gen verwendet) mit dem Ethernet-Protokoll. Die PPP-Protokoll-Information wird innerhalb eines Ethernet-Frames transportiert.
PPTP	Abkürzung für **P**oint to **P**oint **T**unneling **P**rotocol. Eine Spezifikation für VPNs, in denen einige Knoten eines lokalen Netzwerks mit dem Internet verbunden werden.
RADIUS	Abkürzung für **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice Protocol (Dienstprotokoll für entfernte Benutzerauthentisierung im Einwahlverfahren). Ein Internetprotokoll, bei welchem ein Netzwerkserver die Authentisierungs- und Autorisierungsinformationen eines Benutzers, der eine Verbindung herstellen will, von einem Authentisierungsserver erhält.
SA	Abkürzung für **S**ecurity **A**ssociation. Dabei handelt es sich um Security-Policies, welche für die Kommunikation zwischen zwei oder mehreren Systemen definiert wurden. Die Sicherheit der SA wird unter anderem mittels Internet Key Exchange (IKE) gewährleistet.
Smurf	Name einer DoS-Attacke. Bei dieser Attacke verwendet der Angreifer die IP-Adresse des anzugreifenden Systems und sendet ein „Ping“ an die Broadcast-Adresse im Netzwerk. Dieses „Ping“ wird an alle Systeme des entsprechenden Netzwerks weitergeleitet und die Systeme ihrerseits antworten der vermeintlichen Absender-Adresse (IP-Adresse des angegriffenen Systems). Das angegriffene System und das Netzwerk werden auf diese Weise mit Antworten überflutet, was zu Einschränkungen oder einem Unterbruch des Netzwerks und/oder des angegriffenen Systems führen kann.
Sniffer / Packet Sniffer	Zu Deutsch: „Datenpaketschnüffler“. Ein Gerät und/oder ein Programm, das jedes über ein Netzwerk versendete Datenpaket untersucht. Der Sniffer muss dabei innerhalb des Netzwerksegments installiert werden, das untersucht werden soll. Sniffer wurden entwickelt, um die Beseitigung von Problemen zu erleichtern, die die Netzwerkleistung reduzieren. Inzwischen sind Sniffer allerdings auf einigen Netzwerken zum Sicherheitsrisiko geworden, da sie von Hackern eingesetzt werden können, um unverschlüsselte Daten auszuspähen, z.B. Benutzeridentifikationsnummern, Passwörter, Kreditkartennummern, E-Mail-Adressen und andere vertrauliche Daten.
SSL	Abkürzung für **S**ecure **S**ockets **L**ayer. Ein von der Firma Netscape Communications entwickelter offener Standard für den Aufbau sicherer Kommunikationskanäle, die den unberechtigten Zugriff auf sicherheitsrelevante Informationen verhindern sollen. Das Verfahren basiert auf öffentlichen Schlüsseln.
SYN flooding	Name einer DoS-Attacke. Dabei wird das anzugreifende System mit einer Serie von SYN-Paketen überflutet. Auf jedes dieser SYN-Pakete antwortet das angegriffene System mit einem SYN-

	ACK-Paket und wartet auf eine entsprechende Bestätigung (ACK-Paket). Da die Absender-IP-Adresse durch den Angreifer gefälscht wurde, kommt diese Bestätigung jedoch nie zurück. Die Warteschlange für diese halb-offenen Verbindungen füllt sich, was schliesslich dazu führen kann, dass das angegriffene System keine weiteren Verbindungsanfragen, auch nicht von legitimierten Benutzern, mehr entgegen nehmen kann.
Teardrop	Name einer DoS-Attacke. Bei dieser Attacke werden mehrere IP-Paket-Fragmente erzeugt, welche sich überlappen. Diese IP-Pakete werden an das anzugreifende System gesendet. Beim Versuch, die erhaltenen Paket-Fragmente wieder zusammen zu setzen, stürzt das angegriffene System unter Umständen ab oder führt einen Neustart durch.
URL	Abkürzung für **U**niform **R**esource **L**ocator (einheitliche Ressourcenadresse). Eine Adresse für eine Ressource im Internet. URL-Adressen werden von Webbrowsern verwendet, um Internetressourcen zu lokalisieren. Eine URL-Adresse gibt das für den Zugriff auf eine Ressource zu verwendende Protokoll an (z.B. „http://“ für eine Webseite oder „ftp://“ für eine FTP-Site), den Namen des Servers, auf dem sich die Ressource befindet (z.B. „www.hsw.fhz.ch“) sowie – frei wählbar – den Pfad zu einer Ressource (z.B. einem HTML-Dokument oder einer Datei auf diesem Server).
VPN	Abkürzung für **V**irtual **P**rivate **N**etwork. Bestimmte Knoten eines öffentlichen Netzwerks (z.B. des Internets), die sich untereinander mit Hilfe von Verschlüsselungstechnologien und anderen Sicherungsmechanismen verständigen. Durch diese Knoten wird in einem öffentlichen Netzwerk quasi ein Privatnetzwerk integriert. VPNs werden z.B. von Firmen mit mehreren Standorten zur Sicherung des Datenverkehrs zwischen den einzelnen Standorten verwendet.
VPN Transportmodus	Variante eines IPSec VPNs. Beim Transportmodus wird lediglich der Datenteil eines IP-Pakets verschlüsselt, jedoch nicht die Paket-Headerinformationen.
VPN Tunnelmodus	Variante eines IPSec VPNs. Beim Tunnelmodus wird das ganze IP-Paket verschlüsselt, um dieses sicher zu übermitteln. Der Tunnelmodus ist erforderlich, um verschlüsselte VPN-Verbindungen zu internen Systemen herstellen zu können.
WAN	Abkürzung für **W**ide **A**rea **N**etwork. Ein Kommunikationsnetzwerk zur Verbindung geografisch weit getrennter Regionen. Ein WAN besteht oft aus zwei oder mehreren lokalen Netzwerken (LANs). Ein Beispiel für ein WAN ist das Internet.

13. ANHANG

13.1 ZyWALL 10W – Allgemeine interessante Feststellungen bezüglich IT-Sicherheit

13.1.1 Versteckte undokumentierte Datei auf Firewall

Auf der ZyXEL ZyWALL 10W Firewall befindet sich eine undokumentierte und versteckte Datei namens „spt.dat“, in welcher alle wesentlichen Passwörter der Firewall in Klartext gespeichert sind. Obschon diese Datei im Verzeichnis nicht ersichtlich ist, kann sie unter Angabe ihres präzisen Namens mittels FTP von der Firewall heruntergeladen werden:

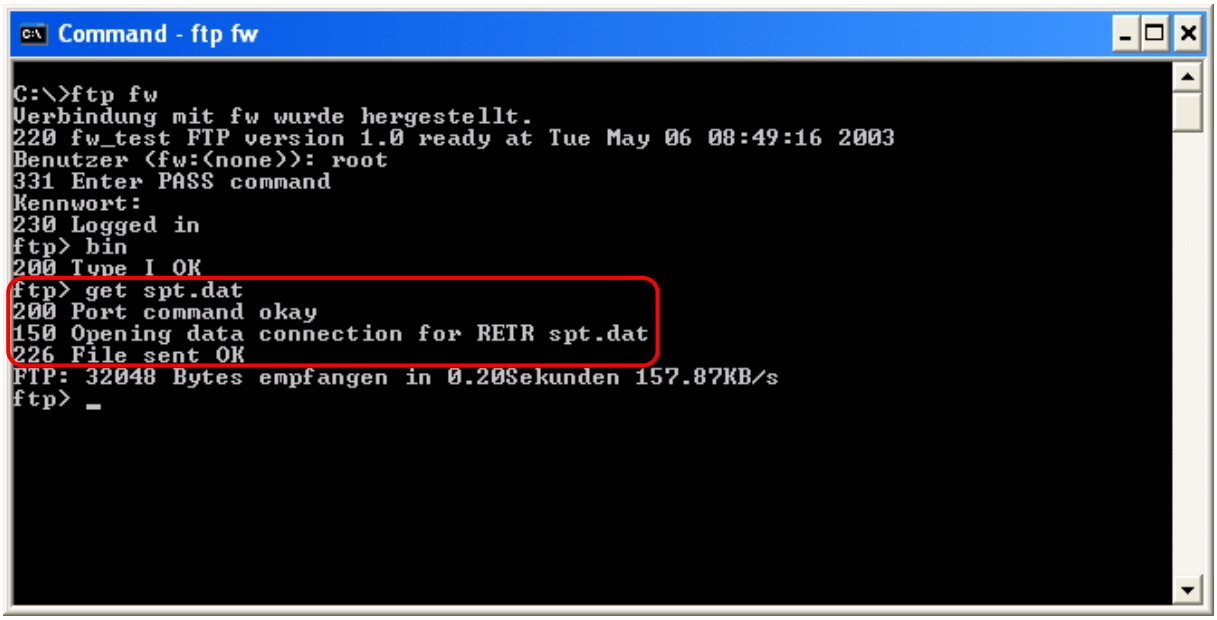

Command - ftp fw
C:\>ftp fw
Verbindung mit fw wurde hergestellt.
220 fw_test FTP version 1.0 ready at Tue May 06 08:49:16 2003
Benutzer (fw:(none)): root
331 Enter PASS command
Kennwort:
230 Logged in
ftp> bin
200 Type I OK
ftp> get spt.dat
200 Port command okay
150 Opening data connection for RETR spt.dat
226 File sent OK
FTP: 32048 Bytes empfangen in 0.20Sekunden 157.87KB/s
ftp> _

Abbildung 41: ZyWALL 10W – Herunterladen der versteckten Datei "spt.dat"

Mit einem Hex-Editor lässt sich der Inhalt der Datei auswerten:

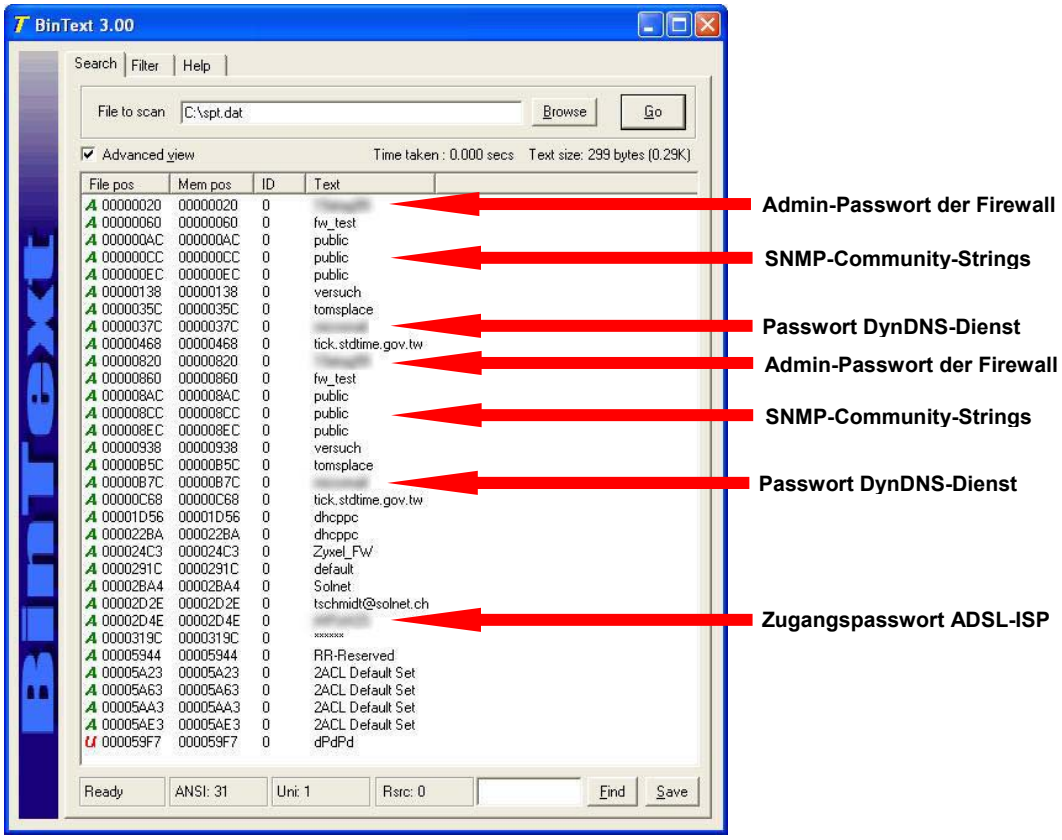


Abbildung 42: ZyWALL 10W – Inhalt der Datei "spt.dat" mit Hex-Editor angezeigt

Es gilt jedoch zu berücksichtigen, dass das Herunterladen dieser versteckten Datei erst möglich ist, nachdem man sich als Administrator am Firewall-FTP-Server angemeldet hat. Somit ist das Risiko eines Missbrauchs dieser Informationen als relativ gering einzuschätzen.

13.1.2 DynDNS-Passwort wird nur schwach codiert über das Internet transferiert

Die Neueröffnung eines Kontos und der Web-Zugriff auf das bestehende Konto beim dynamischen DNS-Dienstanbieter „DynDNS.org“ wird grundsätzlich mittels SSL 128-Bit Verschlüsselung gesichert:

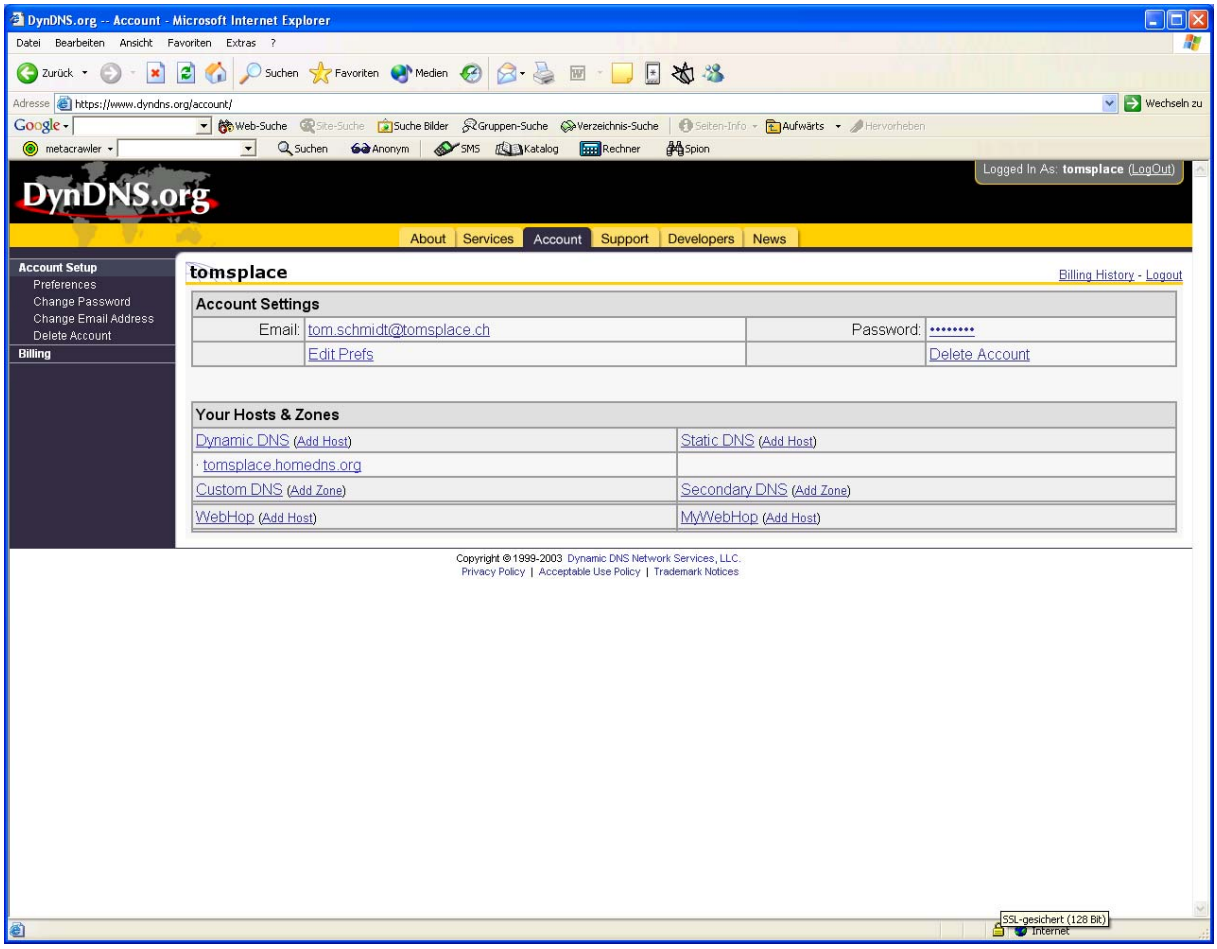


Abbildung 43: DynDNS – Kontozugriff mit SSL-Verschlüsselung

Jedes Mal, wenn das externe Interface der Firewall durch den ISP eine neue dynamische öffentliche IP-Adresse erhält, meldet sich die Firewall beim dynamischen DNS-Anbieter. Dieser eruiert daraufhin die aktuelle öffentliche IP-Adresse des Benutzers. Diese Information wird nun an den dynamischen DNS-Dienst weitergeleitet, um den Eintrag des entsprechenden Benutzers zu aktualisieren. Damit der Eintrag aktualisiert werden kann, muss sich der Benutzer jedoch zuerst am Dienst anmelden. Die Anmeldeinformationen sind in der Firewall hinterlegt und werden automatisch an den Dienst weitergeleitet. Die „Verschlüsselung“ des Passworts erfolgt dabei basierend auf der „Basic-Authorization“-Methode, wobei der Begriff „Verschlüsselung“ hier fehl am Platz ist; das Passwort wird nämlich lediglich mittels Base64 codiert:

```
0000 00 A0 C5 42 EC 7C 00 A0 C5 3E 77 6F 08 00 45 00 ...B.|...>wo..E.
0010 01 39 00 D3 00 00 FE 06 FB 67 C0 A8 00 14 42 97 .9.......g....B.
0020 BC 30 04 0C 00 50 80 C0 00 01 D3 49 95 86 50 18 .0...P.....I..P.
0030 57 80 DC C7 00 00 47 45 54 20 2F 6E 69 63 2F 75 W.....GET /nic/u
0040 70 64 61 74 65 3F 73 79 73 74 65 6D 3D 64 79 6E pdate?system=dyn
0050 64 6E 73 26 68 6F 73 74 6E 61 6D 65 3D 74 6F 6D dns&hostname=tom
0060 73 70 6C 61 63 65 2E 68 6F 6D 65 64 6E 73 2E 6F splace.homedns.o
0070 72 67 26 6D 79 69 70 3D 32 31 32 2E 34 31 2E 36 rg&myip=212.41.6
0080 34 2E 33 32 26 77 69 6C 64 63 61 72 64 3D 4F 4E 4.32&wildcard=ON
0090 26 62 61 63 6B 75 70 6D 78 3D 4E 4F 26 6F 66 66 &backupmx=NO&off
00A0 6C 69 6E 65 3D 4E 4F 20 48 54 54 50 2F 31 2E 31 line=NO HTTP/1.1
00B0 0D 0A 48 6F 73 74 3A 20 6D 65 6D 62 65 72 73 2E ..Host: members.
00C0 64 79 6E 64 6E 73 2E 6F 72 67 0D 0A 41 75 74 68 dyndns.org..Auth
00D0 6F 72 69 7A 61 74 69 6F 6E 3A 20 42 61 73 69 63 orization: Basic
00E0 [redacted]
00F0 [redacted]
0100 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 ontent-Type: app
0110 6C 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 lication/x-www-f
0120 6F 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A orm-urlencoded..
0130 55 73 65 72 2D 41 67 65 6E 74 3A 20 52 41 53 2F User-Agent: RAS/
0140 31 2E 31 0D 0A 0D 0A                           1.1....
```

Base64-codiertes Passwort

Abbildung 44: DynDNS – Sniffer-Output der Anmeldeinformationen mit Base64-codiertem Passwort

Das mit einem Sniffer abgefangene Paket mit den Anmeldeinformationen für den dynamischen DNS-Dienst kann problemlos mit einem Base64-Decoder wieder in Klartext zurückübersetzt werden:

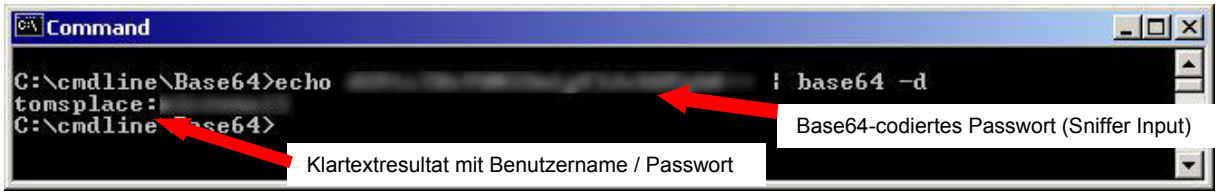
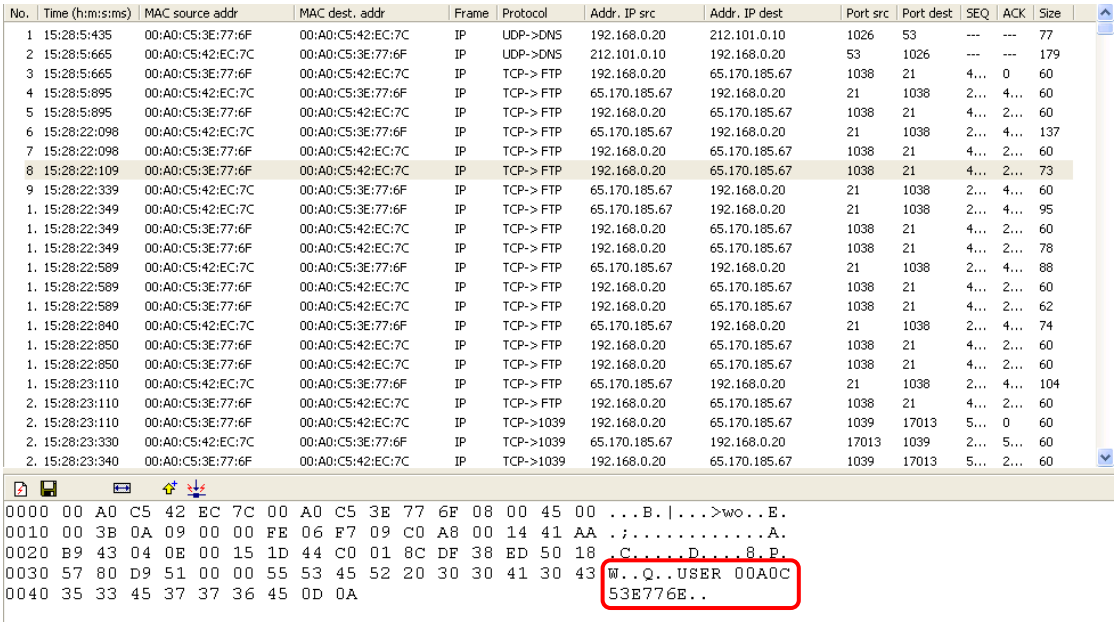


Abbildung 45: DynDNS – Decodieren des Base64-codierten Passworts

Aufgrund der SSL-Verschlüsselung auf der Website des dynamischen DNS-Anbieters „DynDNS.org“ wiegen sich viele Benutzer in falscher Sicherheit. Sie gehen davon aus, dass ihr Passwort stark verschlüsselt über das Internet übertragen wird, was beim Zugriff über den Web-Server von „DynDNS.org“ dank SSL ja auch der Fall ist. Dass ihr Passwort beim Aktualisieren der neuen dynamischen IP-Adresse jedoch lediglich Base64-codiert übermittelt wird, ist wahrscheinlich den wenigsten Benutzern bewusst (und die Aktualisierung des Eintrags erfolgt sicher viel häufiger als der Web-Zugriff auf das Konto…).

13.1.3 Ergebnisse technische Untersuchungen URL-Filtering ZyWALL 10W

Um die Filter-Listen-Updatefunktion des URL-Filtering näher untersuchen zu können, wurde der entsprechende Netzwerkverkehr WAN-seitig mit einem Sniffer analysiert. Bei einem Filter-Listen-Update baut die Firewall eine FTP-Verbindung zur IP-Adresse 65.170.185.67 auf. Der FTP-Zugang ist passwortgeschützt und die Firewall übermittelt den benötigten Usernamen (siehe Abbildung 46) und das Passwort automatisch.

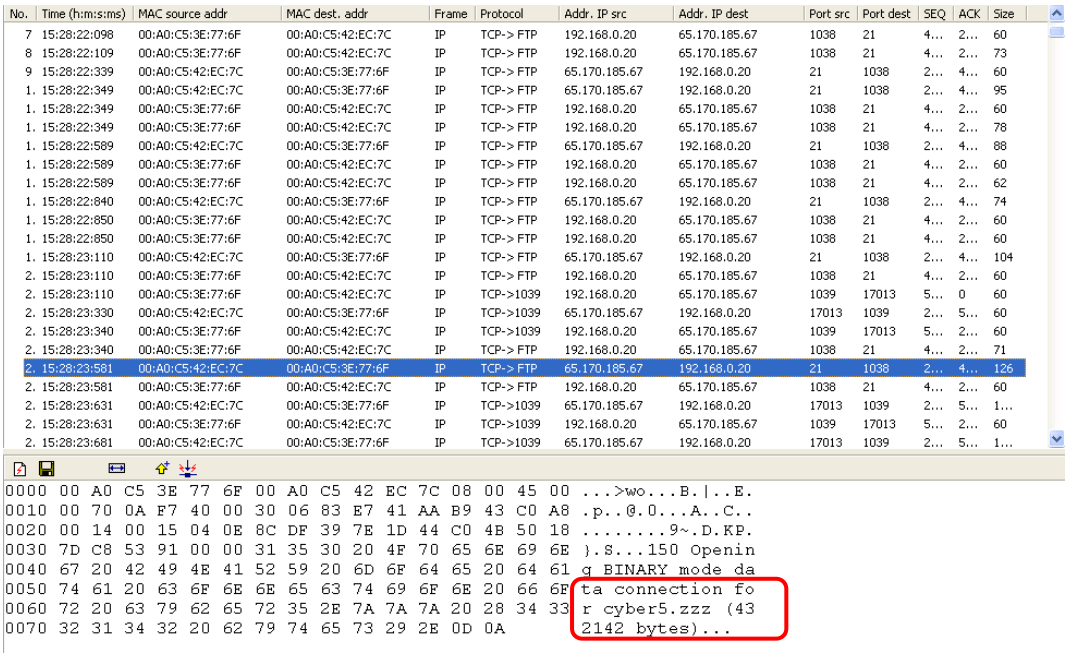


No.	Time (h:m:s:ms)	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP src	Addr. IP dest	Port src	Port dest	SEQ	ACK	Size
1	15:28:5:435	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	UDP->DNS	192.168.0.20	212.101.0.10	1026	53	---	---	77
2	15:28:5:665	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	UDP->DNS	212.101.0.10	192.168.0.20	53	1026	---	---	179
3	15:28:5:665	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	0	60
4	15:28:5:895	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	60
5	15:28:5:895	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
6	15:28:22:098	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	137
7	15:28:22:098	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
8	15:28:22:109	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	73
9	15:28:22:339	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	60
1.	15:28:22:349	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	95
1.	15:28:22:349	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:22:349	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	78
1.	15:28:22:589	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	88
1.	15:28:22:589	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:22:589	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	62
1.	15:28:22:840	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	74
1.	15:28:22:850	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:22:850	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:23:110	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	104
2.	15:28:23:110	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
2.	15:28:23:110	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP->1039	192.168.0.20	65.170.185.67	1039	17013	5...	0	60
2.	15:28:23:330	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP->1039	65.170.185.67	192.168.0.20	17013	1039	2...	5...	60
2.	15:28:23:340	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP->1039	192.168.0.20	65.170.185.67	1039	17013	5...	2...	60

```
0000 00 A0 C5 42 EC 7C 00 A0 C5 3E 77 6F 08 00 45 00 ...B.|...>wo..E.
0010 00 3B 0A 09 00 00 FE 06 F7 09 C0 A8 00 14 41 AA .;............A.
0020 B9 43 04 0E 00 15 1D 44 C0 01 8C DF 38 ED 50 18 .C.....D....8.P.
0030 57 80 D9 51 00 00 55 53 45 52 20 30 30 41 30 43 W..Q..USER 00A0C
0040 35 33 45 37 37 36 45 0D 0A                      53E776E..
```

Abbildung 46: ZyWALL 10W – Übermittelter Benutzername für das URL-Filtering-Update

Nach der erfolgreichen Authentisierung wird eine passive FTP-Verbindung aufgebaut und die Filter-Liste (Datei „cyber5.zzz“) wird auf die Firewall heruntergeladen:



No.	Time (h:m:s:ms)	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP src	Addr. IP dest	Port src	Port dest	SEQ	ACK	Size
7	15:28:22:098	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
8	15:28:22:109	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	73
9	15:28:22:339	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	60
1.	15:28:22:349	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	95
1.	15:28:22:349	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:22:349	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	78
1.	15:28:22:589	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	88
1.	15:28:22:589	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:22:589	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	62
1.	15:28:22:840	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	74
1.	15:28:22:850	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:22:850	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
1.	15:28:23:110	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	104
2.	15:28:23:110	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
2.	15:28:23:110	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP->1039	192.168.0.20	65.170.185.67	1039	17013	5...	0	60
2.	15:28:23:330	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP->1039	65.170.185.67	192.168.0.20	17013	1039	2...	5...	60
2.	15:28:23:340	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP->1039	192.168.0.20	65.170.185.67	1039	17013	5...	2...	60
2.	15:28:23:340	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	71
2.	15:28:23:581	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP-> FTP	65.170.185.67	192.168.0.20	21	1038	2...	4...	126
2.	15:28:23:581	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP-> FTP	192.168.0.20	65.170.185.67	1038	21	4...	2...	60
2.	15:28:23:631	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP->1039	65.170.185.67	192.168.0.20	17013	1039	2...	5...	1...
2.	15:28:23:631	00:A0:C5:3E:77:6F	00:A0:C5:42:EC:7C	IP	TCP->1039	192.168.0.20	65.170.185.67	1039	17013	5...	2...	60
2.	15:28:23:681	00:A0:C5:42:EC:7C	00:A0:C5:3E:77:6F	IP	TCP->1039	65.170.185.67	192.168.0.20	17013	1039	2...	5...	1...

```
0000 00 A0 C5 3E 77 6F 00 A0 C5 42 EC 7C 08 00 45 00 ...>wo...B.|..E.
0010 00 70 0A F7 40 00 30 06 83 E7 41 AA B9 43 C0 A8 .p..@.0...A..C..
0020 00 14 00 15 04 0E 8C DF 39 7E 1D 44 C0 4B 50 18 ........9~.D.KP.
0030 7D C8 53 91 00 00 31 35 30 20 4F 70 65 6E 69 6E }.S...150 Openin
0040 67 20 42 49 4E 41 52 59 20 6D 6F 64 65 20 64 61 g BINARY mode da
0050 74 61 20 63 6F 6E 6E 65 63 74 69 6F 6E 20 66 6F ta connection fo
0060 72 20 63 79 62 65 72 35 2E 7A 7A 7A 20 28 34 33 r cyber5.zzz (43
0070 32 31 34 32 20 62 79 74 65 73 29 2E 0D 0A       2142 bytes)...
```

Abbildung 47: ZyWALL 10W – URL-Filter-Datei

Aufgrund des mit dem Sniffer eruierten Benutzernamen und Passwortes besteht jedoch die Möglichkeit, mittels FTP-Client direkt eine Verbindung auf den FTP-Filter-Update-Server herzustellen. Nach dem Aufbau der entsprechenden Verbindung befindet man sich im Verzeichnis „/usr/ftpSQL“. Wie in der Abbildung 48 ersichtlich ist, sind in diesem Verzeichnis nicht nur die durch die Firewall heruntergeladene Datei „cyber5.zzz“, sondern auch noch weitere Dateien vorhanden, mit welchen zum Teil die Filter-Listen aufbereitet werden. In den

beiden PDF-Dateien ist zudem ersichtlich, dass die Filter-Liste auf dem Produkt „Cyber Patrol“ basiert.

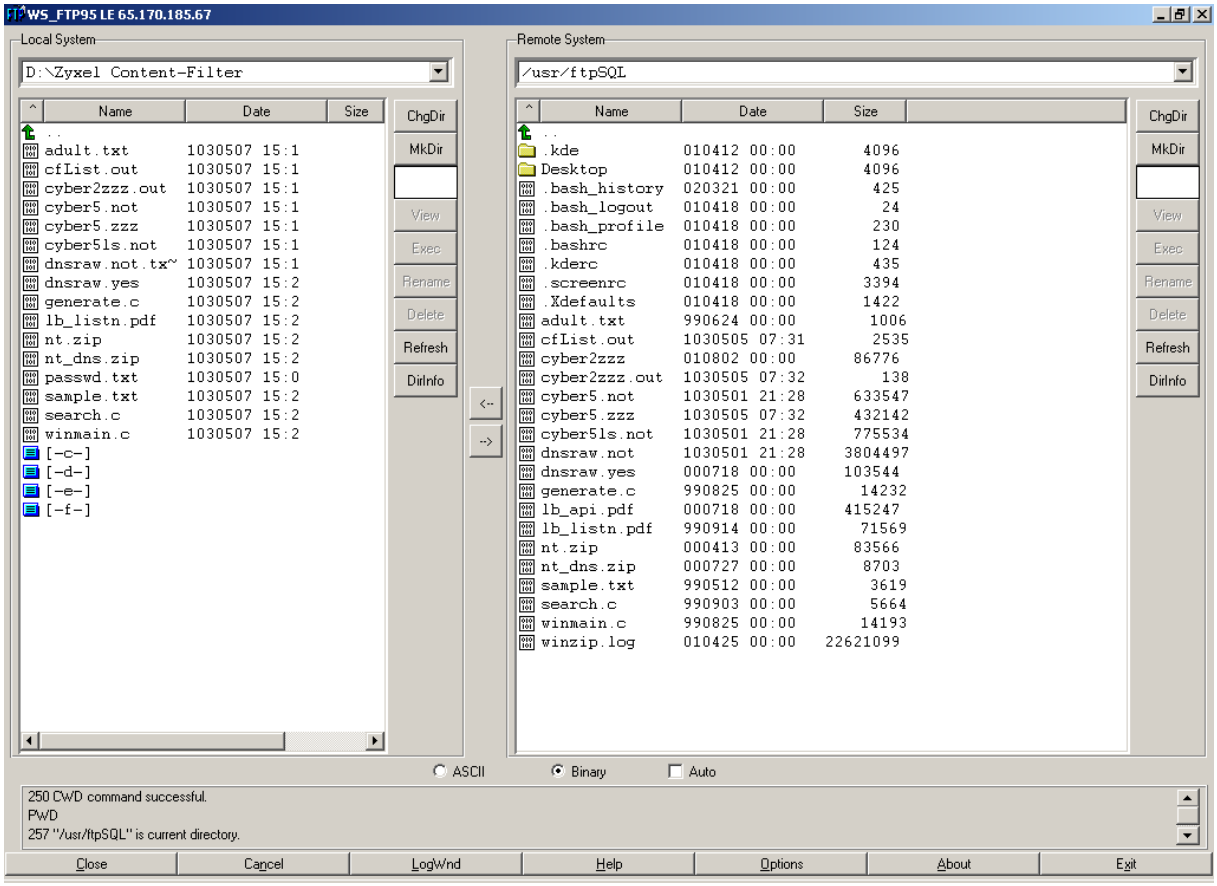


Abbildung 48: ZyWALL 10W – Inhalt des URL-Filter-Update-Verzeichnisses

Bei einer der Quelldateien handelt es sich um die Datei „dnsraw.not“ (Abbildung 49), welche die zu filternden Webseiten im RAW-Format beinhaltet:

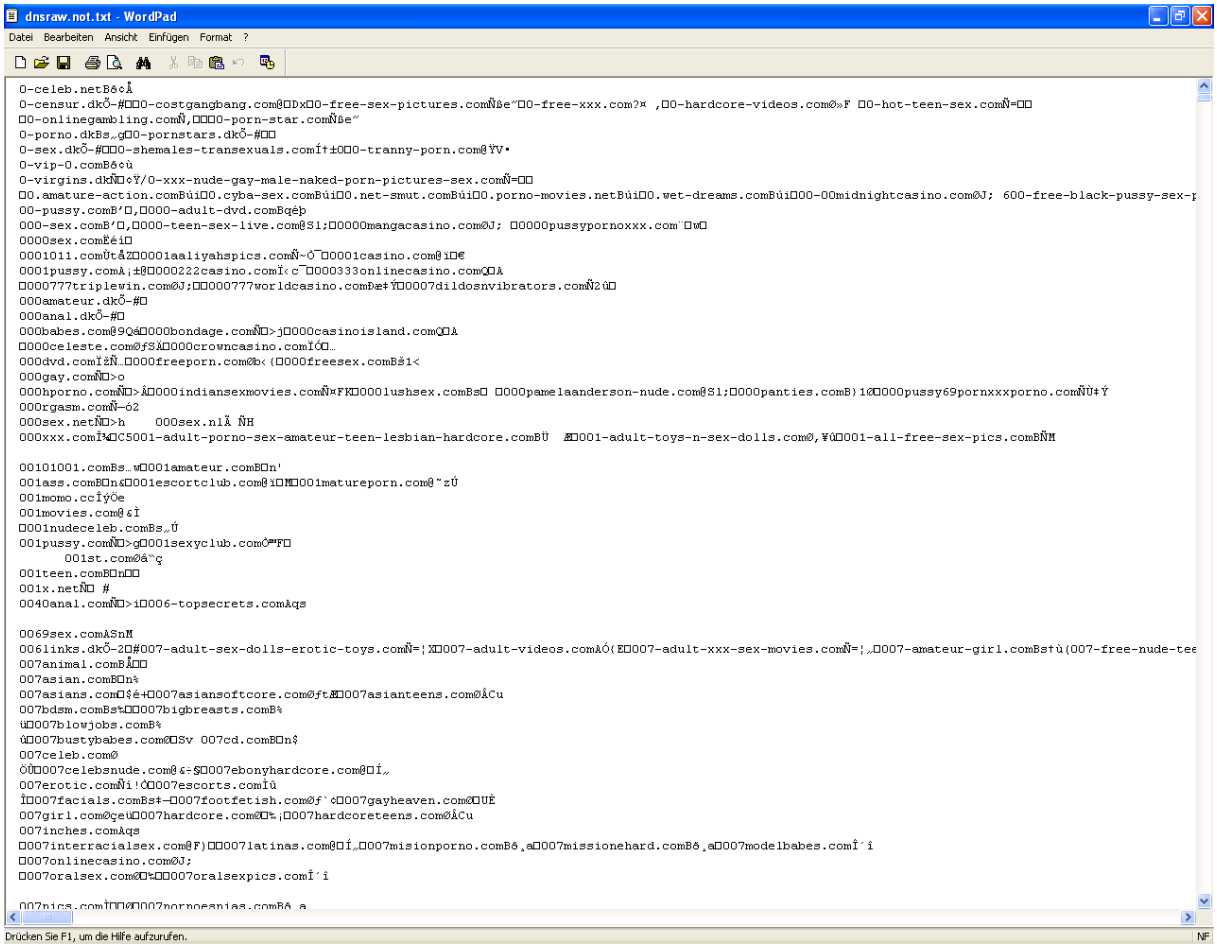


Abbildung 49: ZyWALL 10W – Inhalt der URL-Filter-Liste

Und zu guter letzt, wenn man sich nun bereits auf einem FTP-Server befindet, liegt der Versuch nahe (Abbildung 50) auszutesten, ob man eventuell auch auf andere interessante Dateien Zugriff hat... ;-)

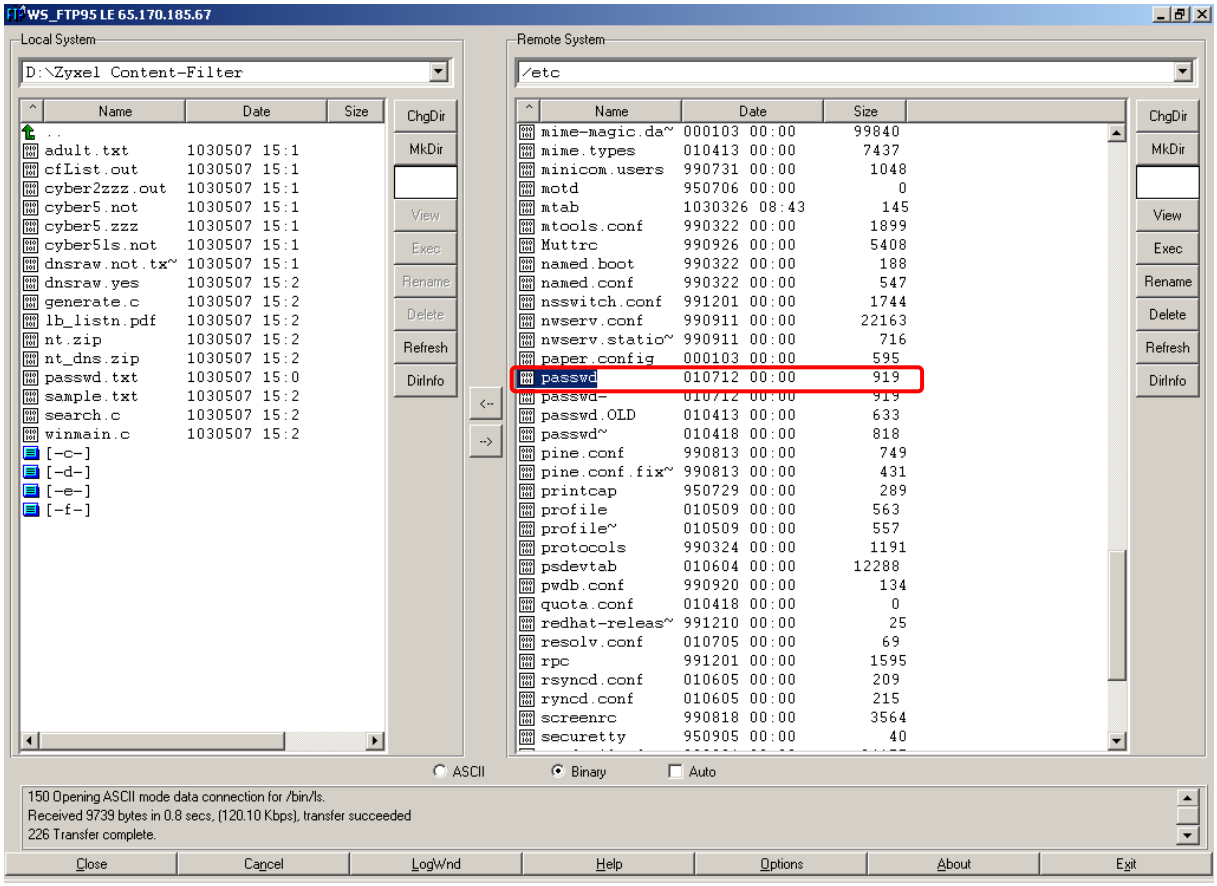


Abbildung 50: ZyWALL 10W – Zugriff auf die Datei "/etc/passwd" des FTP-Servers

13.2 Konfigurationsbeispiele

13.2.1 Bridging-Modus-Konfiguration des ZyXEL Prestige 642R ADSL-Routers

Falls sich die ZyXEL ZyWALL 10W Firewall hinter einem ADSL-Router befindet und das externe Interface der Firewall anstelle des externen Interface des ADSL-Routers die dynamische öffentliche IP-Adresse des ISP erhalten soll (z.B. um einen dynamischen DNS-Dienst nutzen zu können), ist eine Umkonfiguration des ADSL-Routers nötig. Die dazu erforderlichen Schritte werden nachfolgend anhand der Konfiguration eines ZyXEL Prestige 642R ADSL-Routers erläutert:

Im Menu 1 (General Setup) des Routers die Einstellung „Route IP“ von „Yes“ auf „No“ und die Einstellung „Bridge“ von „No“ auf „Yes“ setzen. Das Resultat sollte danach folgendermassen aussehen:

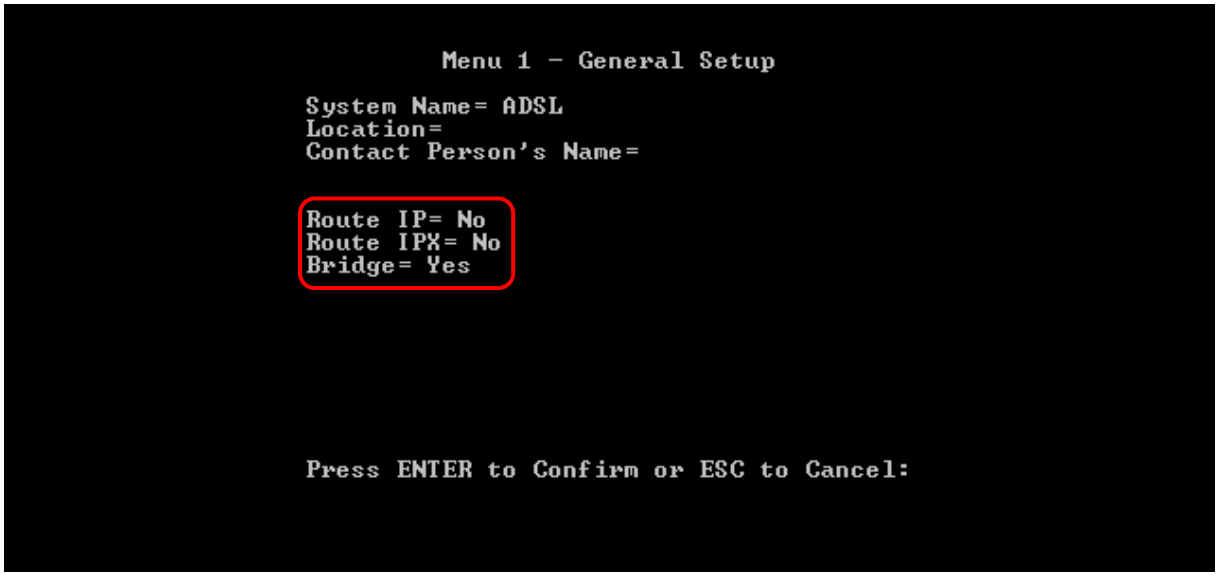


Abbildung 51: ZyXEL Prestige 642R – Menu 1 (General Setup)

Im Menu 4 (Internet Access Setup) des Routers die Einstellung „Encapsulation“ von „PPPoE“ auf „RFC 1483“ setzen:

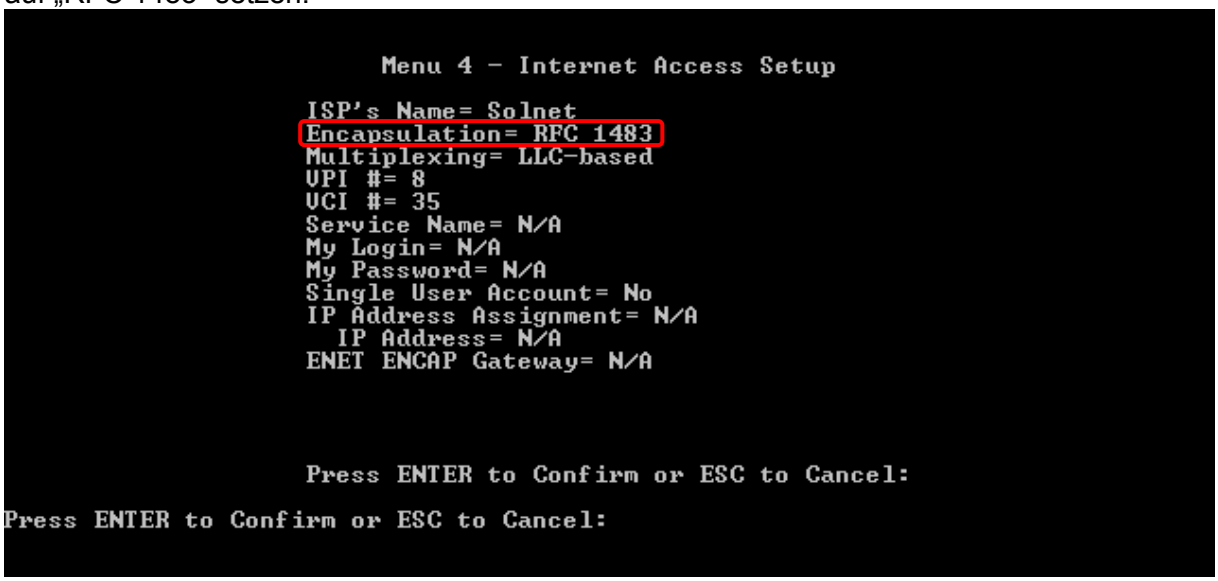

Menu 4 - Internet Access Setup
ISP's Name= Solnet
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
Service Name= N/A
My Login= N/A
My Password= N/A
Single User Account= No
IP Address Assignment= N/A
IP Address= N/A
ENET ENCAP Gateway= N/A
Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:

Abbildung 52: ZyXEL Prestige 642R – Menu 4 (Internet Access Setup)

Im Menu 11.1 (Remote Node Setup / Profile) des Routers die Einstellung „Route“ von „IP“ auf „None“ und die Einstellung „Bridge“ von „No“ auf „Yes“ setzen, was zu folgenden Resultat führt:

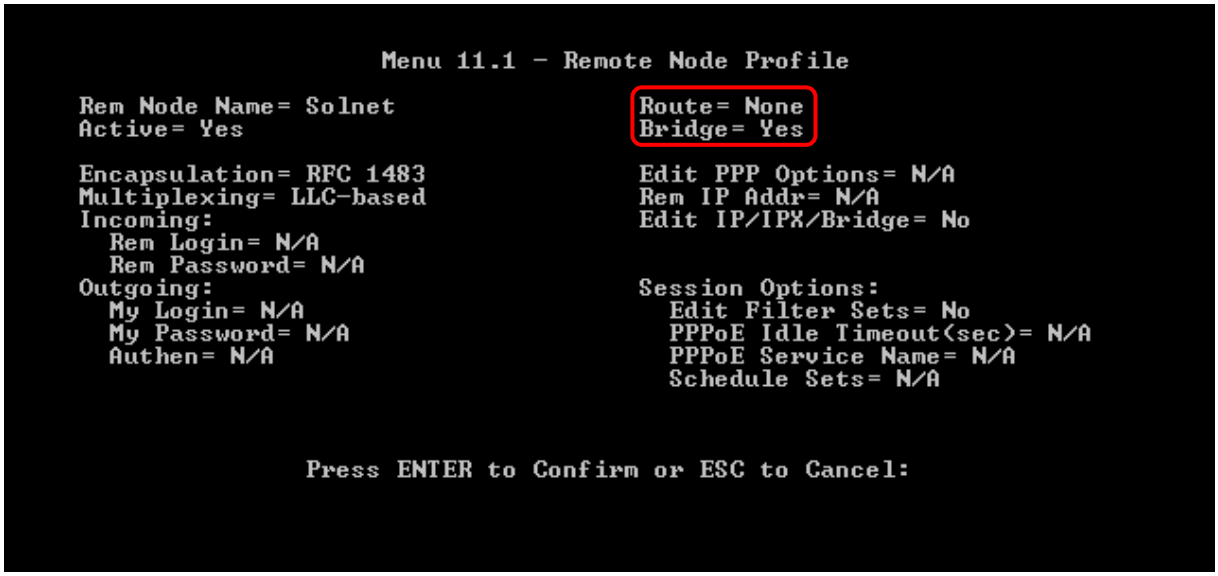


Abbildung 53: ZyXEL Prestige 642R – Menu 11.1 (Remote Node Profile)

Mit diesen Einstellungen befindet sich der ADSL-Router nun im Bridging-Modus und die dynamische öffentliche IP-Adresse des ISP wird dadurch direkt dem externen Interface der Firewall zugewiesen.

13.2.2 ZyWALL 10W – VPN-Einstellungen für die Interoperabilität mit SonicWALL SOHO 3 und Check Point Firewall-1 NG

VPN-Einstellungen für die VPN-Verbindung mit der SonicWALL SOHO3 Firewall:

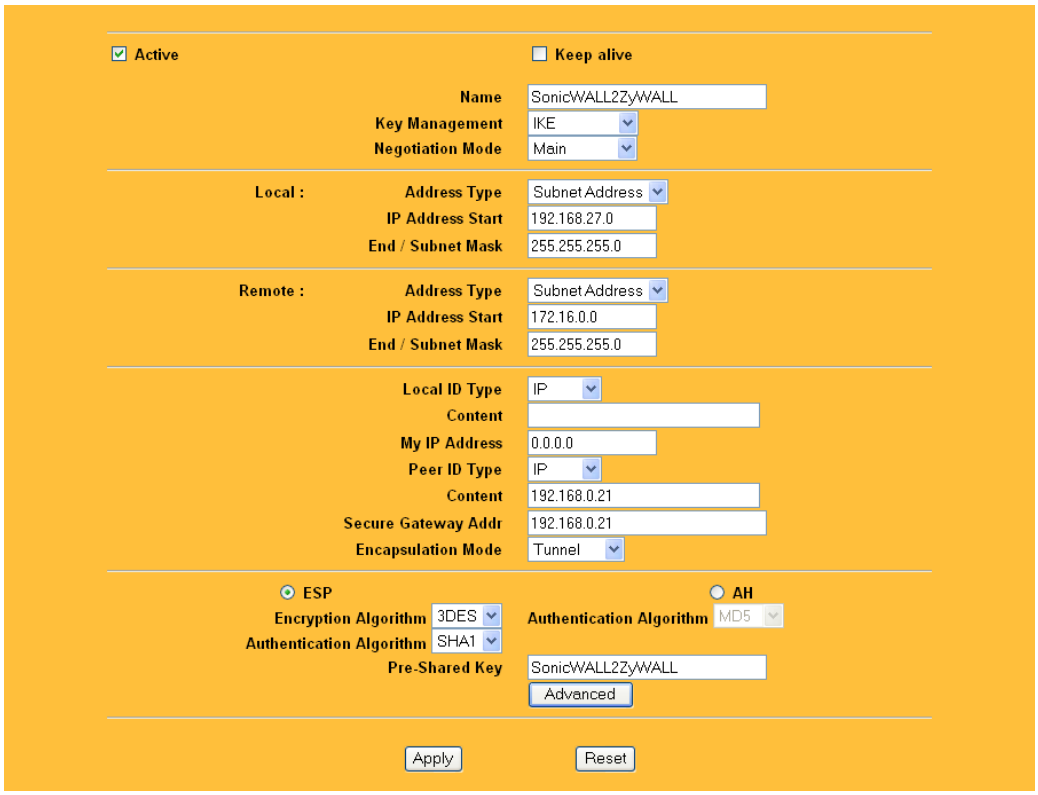


Abbildung 54: ZyWALL 10W – VPN-Grundeinstellungen für VPN-Verbindung mit der SonicWALL SOHO3

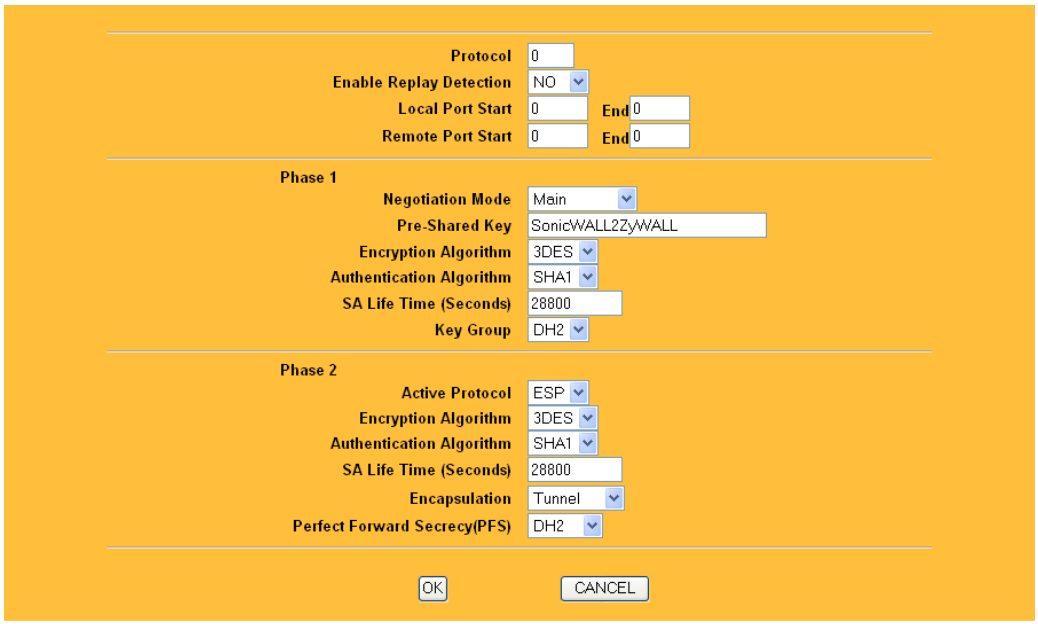


Abbildung 55: ZyWALL 10W – Erweitere VPN-Einstellungen für VPN-Verbindung mit der SonicWALL SOHO3

VPN-Einstellungen für die VPN-Verbindung mit der Check Point Firewall-1 NG Firewall:

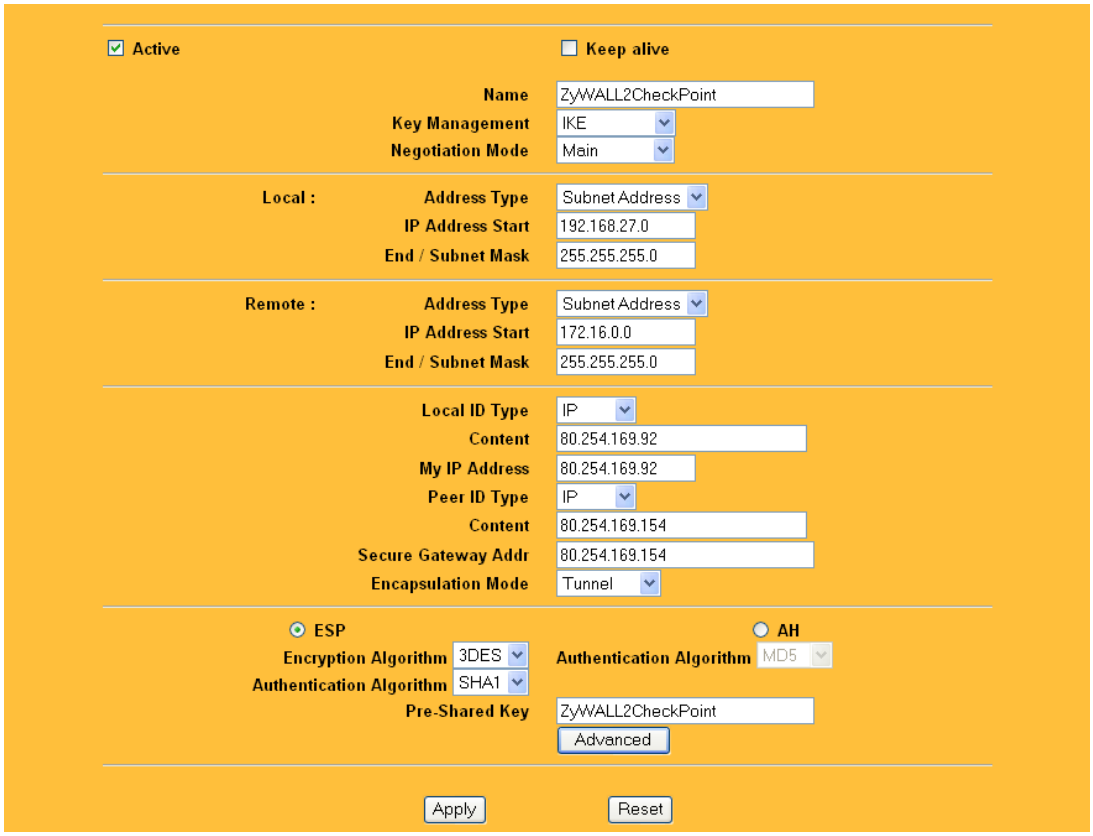


Abbildung 56: ZyWALL 10W – VPN-Grundeinstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG

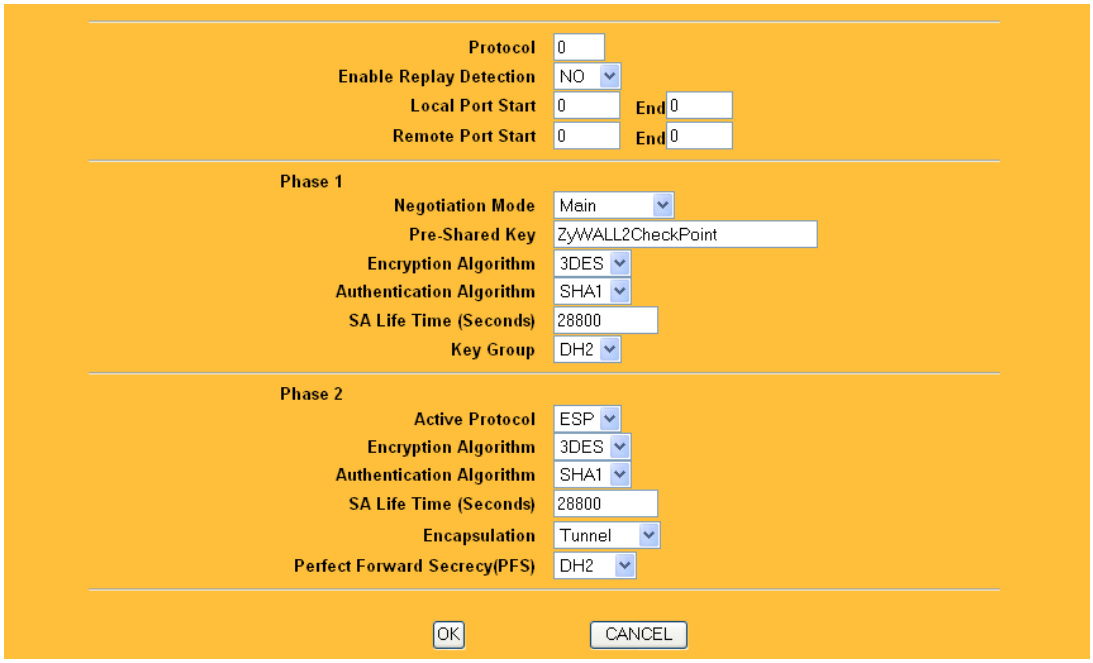


Abbildung 57: ZyWALL 10W – Erweitere VPN-Einstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG

13.2.3 SonicWALL SOHO3 – VPN-Einstellungen für die Interoperabilität mit ZyWALL 10W und Check Point Firewall-1 NG

VPN-Einstellungen für die VPN-Verbindung mit der ZyWALL 10W Firewall:

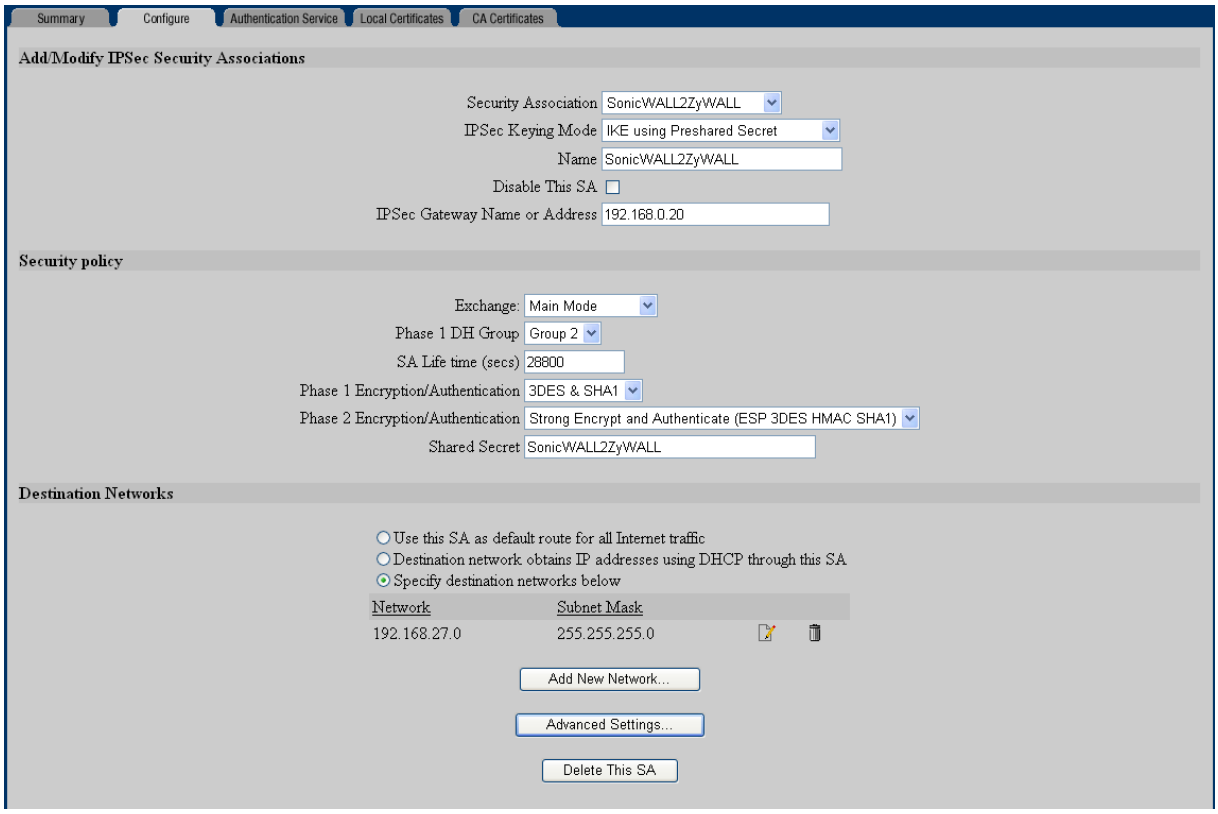


Abbildung 58: SonicWALL SOHO3 – VPN-Grundeinstellungen für VPN-Verbindung mit der ZyWALL 10W

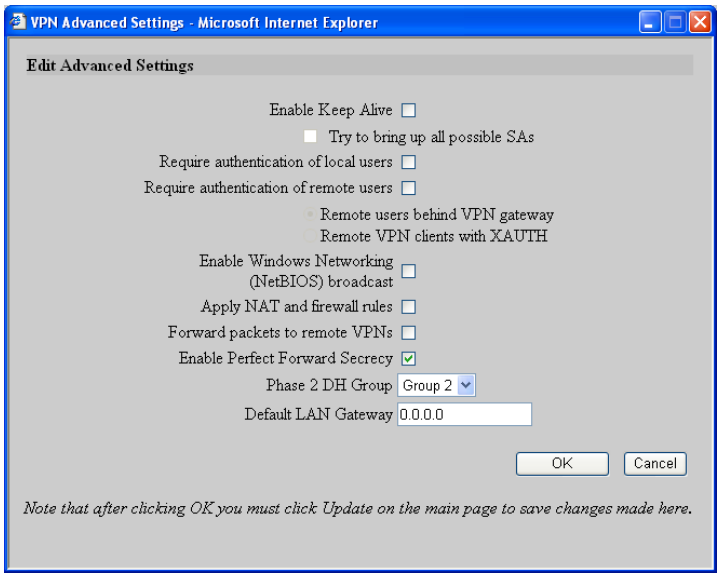

VPN Advanced Settings - Microsoft Internet Explorer
Edit Advanced Settings
Enable Keep Alive
Try to bring up all possible SAs
Require authentication of local users
Require authentication of remote users
Remote users behind VPN gateway
Remote VPN clients with XAUTH
Enable Windows Networking (NetBIOS) broadcast
Apply NAT and firewall rules
Forward packets to remote VPNs
Enable Perfect Forward Secrecy
Phase 2 DH Group
Group 2
Default LAN Gateway
0.0.0.0
OK
Cancel
Note that after clicking OK you must click Update on the main page to save changes made here.

Abbildung 59: SonicWALL SOHO3 – Erweitere VPN-Einstellungen für VPN-Verbindung mit der ZyWALL 10W

VPN-Einstellungen für die VPN-Verbindung mit der Check Point Firewall-1 NG Firewall:

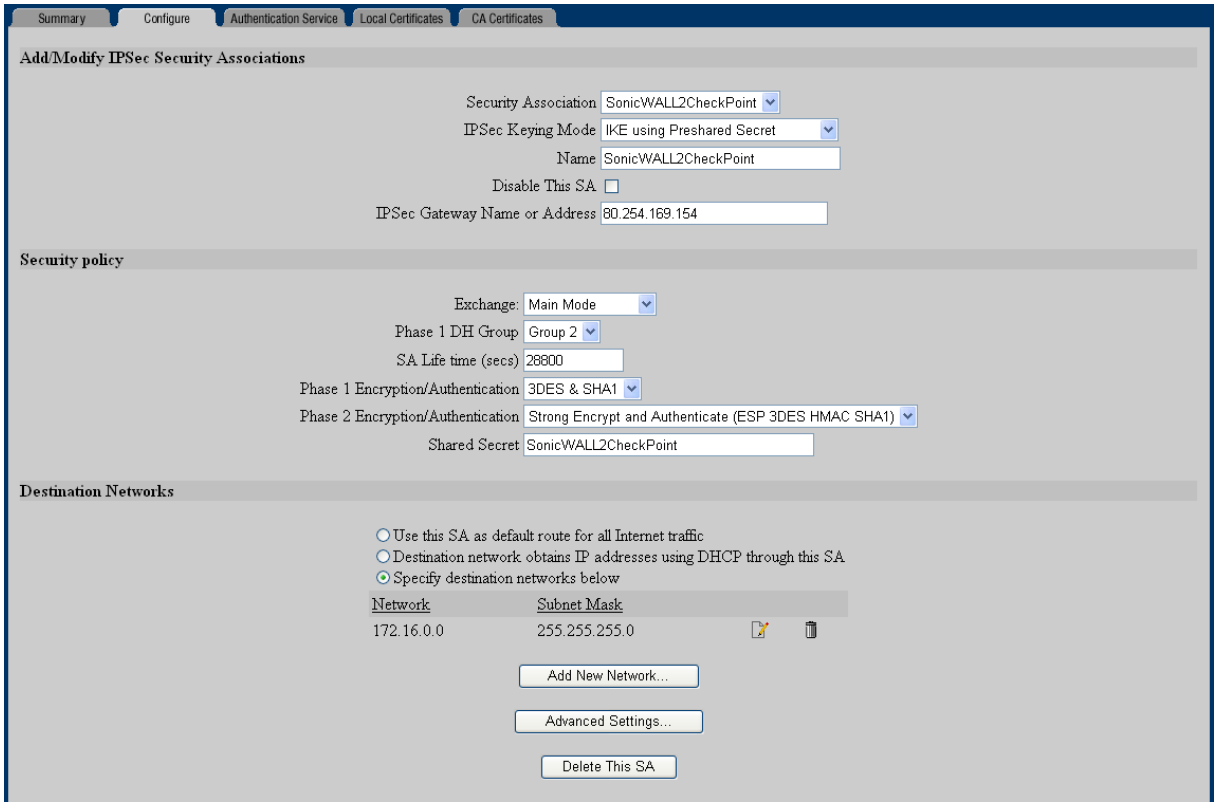


Abbildung 60: SonicWALL SOHO3 – VPN-Grundeinstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG

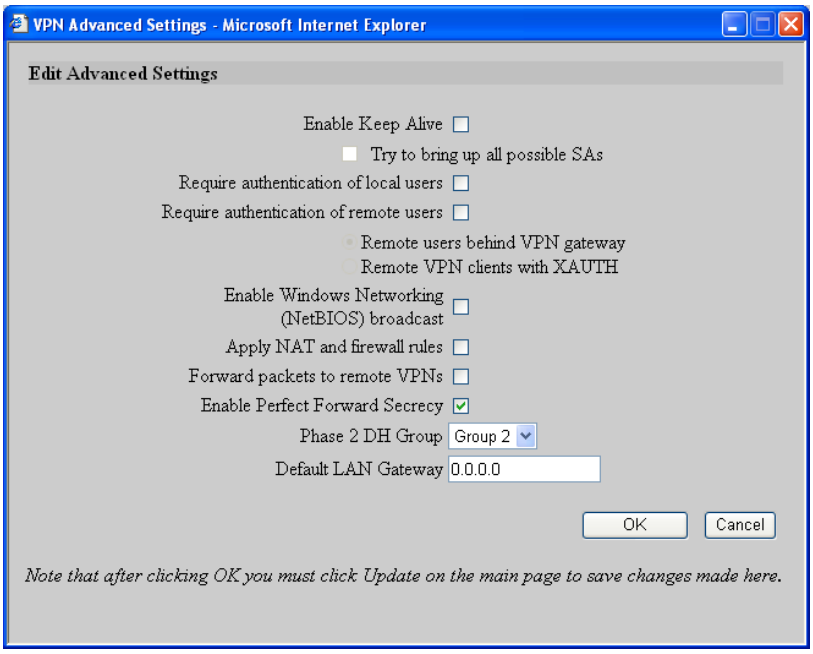
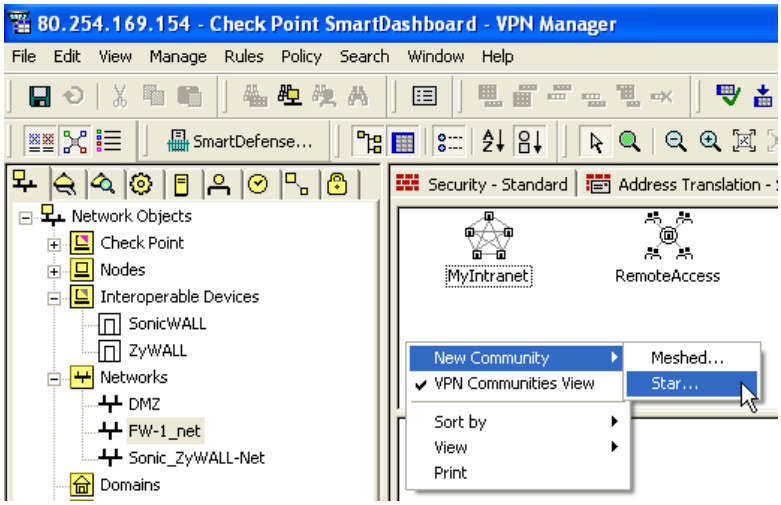

VPN Advanced Settings - Microsoft Internet Explorer
Edit Advanced Settings
Enable Keep Alive
Try to bring up all possible SAs
Require authentication of local users
Require authentication of remote users
Remote users behind VPN gateway
Remote VPN clients with XAUTH
Enable Windows Networking (NetBIOS) broadcast
Apply NAT and firewall rules
Forward packets to remote VPNs
Enable Perfect Forward Secrecy
Phase 2 DH Group
Group 2
Default LAN Gateway
0.0.0.0
OK
Cancel
Note that after clicking OK you must click Update on the main page to save changes made here.

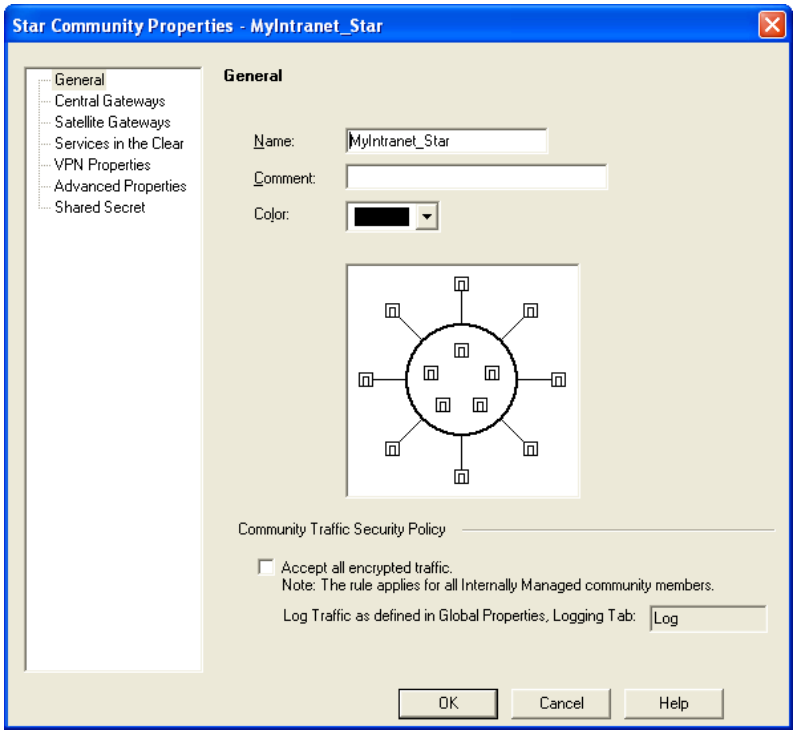
Abbildung 61: SonicWALL SOHO3 – Erweitere VPN-Einstellungen für VPN-Verbindung mit der Check Point Firewall-1 NG

13.2.4 Check Point Firewall-1 NG – VPN-Einstellungen für die Interoperabilität mit ZyWALL 10 W und SonicWALL SOHO 3

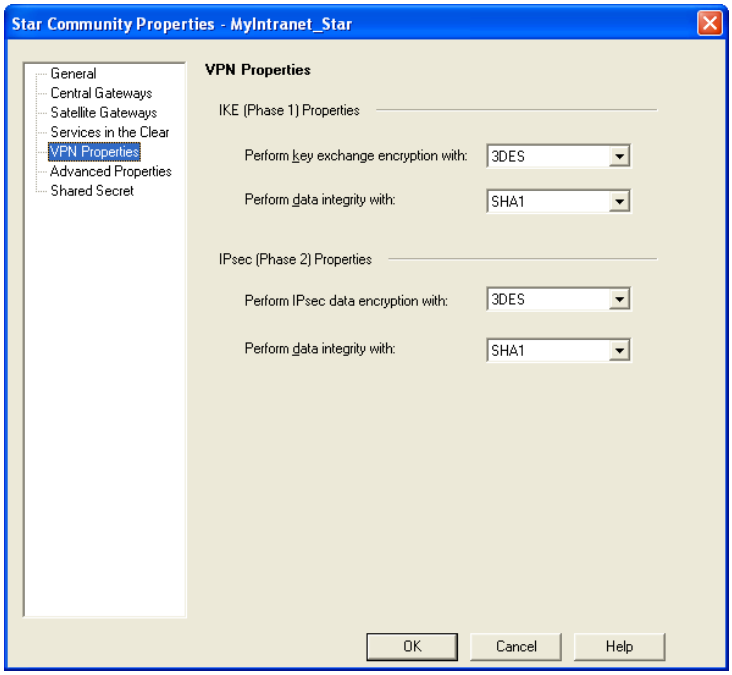
Auf der Check Point Firewall-1 NG FP 3 müssen folgende Einstellungen vorgenommen werden:

- Aktivierung des VPN-Moduls „VPN-1 Pro“ in den „General Properties“ der Firewall
- Folgende Objekte erstellen:
  - Objekt-Typ „Network“ ⇨ Name „Sonic_ZyWALL-Net“ ⇨ Netzwerk-Adresse „192.168.27.0“ ⇨ Netzmaske „255.255.255.0“ ⇨ Broadcast-Adresse „included“
  - Objekt-Typ „Network“ ⇨ Name „FW-1-Net“ ⇨ Netzwerk-Adresse „172.16.0.0“ ⇨ Netzmaske „255.255.255.0“ ⇨ Broadcast-Adresse „included“
  - Objekt-Typ „Interoperable Device“ ⇨ Name „ZyWALL“ ⇨ IP-Adresse „80.254.169.92“ ⇨ Topology – VPN Domain – Manually defined „Sonic_ZyWALL-Net“
  - Objekt-Typ „Interoperable Device“ ⇨ Name „SonicWALL” ⇨ IP-Adresse „80.254.169.90“ ⇨ Topology – VPN Domain – Manually defined „Sonic_ZyWALL-Net“
- Im „VPN Manager“ mittels Doppelklick auf das Objekt „MyIntranet“ die vorhandene „Meshed-Community“ verwenden oder aber mittels rechter Maustaste eine neue VPN-Community erstellen (im folgenden Konfigurationsbeispiel wird eine neue Star-Community erstellt):

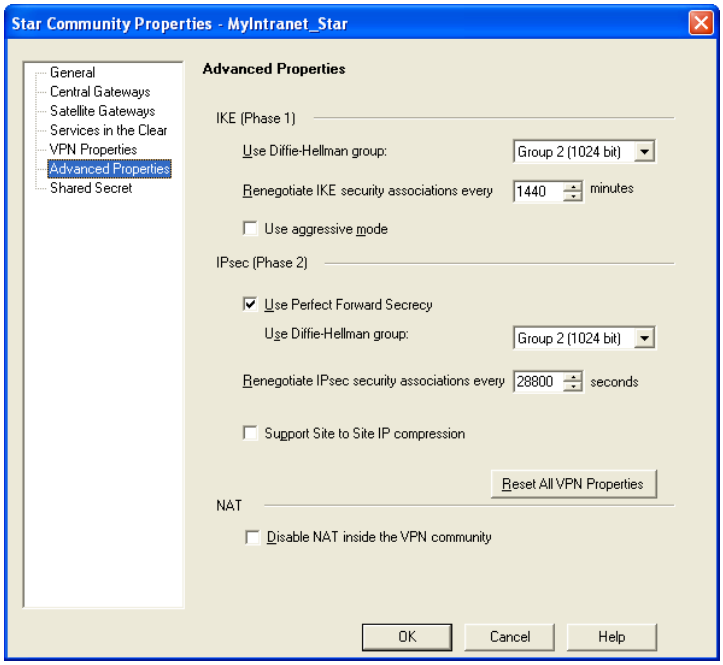




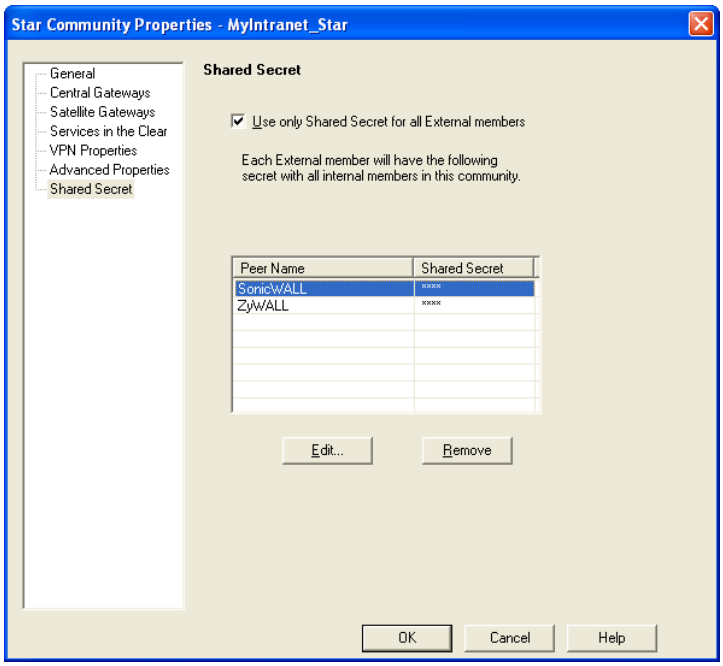
- Unter „Central Gateways“ das Firewall-Objekt auswählen
- Unter „Satellite Gateways“ die beiden Objekte „ZyWALL“ und „SonicWALL“
- Unter „VPN Properties“ folgende Einstellungen vornehmen:



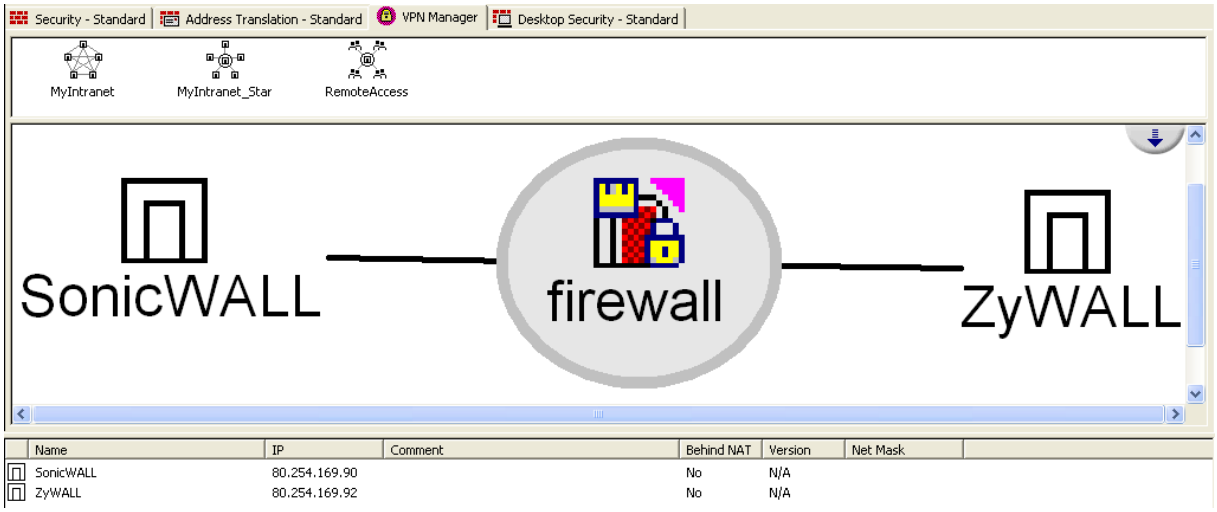
- Unter „Advanced Properties“ folgende Einstellungen vornehmen:



- Unter „Shared Secret“ die auf der ZyWALL und SonicWALL definierten „Preshared-Secret“-Passwörter eingeben:



Das Ergebnis sieht danach folgendermassen aus:



Damit die internen Netzwerke hinter den beiden Firewalls miteinander kommunizieren können, müssen noch entsprechende Firewall-Regeln auf der Check Point Firewall-1 NG erfasst werden. Es gilt zu beachten, dass dafür eigentlich nur die Firewall-Regel Nr. 3 benötigt wird. Die beiden anderen Regeln wurden lediglich als Anschauungsbeispiel erfasst:

Erläuterungen zu den abgebildeten Regeln

Nr.	Erläuterungen
1	Alle Verbindungen, welche Bestandteil der VPN-Community „MyIntranet_Star“ sind (siehe „IF VIA“), können auf die Firewall zugreifen. Mit der Regel-Einschränkung über „IF VIA“ lassen sich elegant Zugriffe für an VPN-Communities beteiligte Netzwerke und Systeme definieren.
2	Alle übrigen Verbindungen und Systeme haben keinen Zugriff auf die Firewall (Stealth-Regel)
3	Die internen Netzwerke hinter den beiden Firewalls können miteinander uneingeschränkt kommunizieren

13.2.5 Windows 2000 IPSec – VPN-Client für Firewalls „selbst gemacht“

Wenn auf der Firewall VPN eingerichtet wurde, besteht die Möglichkeit, nicht nur Firewall-zu-Firewall-Verbindungen mittels VPN herzustellen, sondern auch mit einer Arbeitsstation eine VPN-Verbindung zur Firewall aufzubauen. Dazu wird ein so genannter VPN-Client benötigt. Da weder mit der ZyXEL ZyWALL 10W noch mit der SonicWALL SOHO3 ein solcher mitgeliefert wird, muss man entweder auf ein kostenpflichtiges Produkt zurückgreifen (Produkt direkt vom Firewall-Hersteller, wie z.B. bei SonicWALL, oder Drittprodukt) oder man konfiguriert sich mit den „Bordmitteln“ von Windows 2000 selber einen VPN-Client, welcher sowohl für die ZyWALL- als auch für die SonicWALL-Firewall eingesetzt werden kann.

Auf den folgenden Seiten befindet sich eine Schritt-für-Schritt-Anleitung, wie ein solcher VPN-Client unter Windows 2000 konfiguriert wird. Die Anleitung besteht primär aus

Screenshots (auf eine Beschriftung jedes einzelnen Screenshots wurde dabei absichtlich verzichtet); auf diesen ist ersichtlich, bei welcher Maske welche Eingaben vorgenommen werden müssen. Der abgebildete Mauszeiger zeigt immer an, welche Schaltfläche als nächstes betätigt werden muss. Teilweise werden kurze Erläuterungen oder Kommentare den Screenshots hinzugefügt.

Diese Schritt-für-Schritt-Anleitung lässt sich übrigens auch für eine VPN-Client-Anbindung an eine Check Point Firewall-1 NG FP 3 Firewall verwenden. Damit die Verbindung jedoch klappt, muss mit digitalen Zertifikaten gearbeitet werden. An der entsprechenden Stelle in der folgenden Anleitung wird auf diesen Umstand mit einem Verweis auf das nächste Kapitel hingewiesen, in welchem für die abweichenden Punkte eine kurze Anleitung für Check Point Firewalls zu finden ist (siehe Kapitel 13.2.6).

Für die Konfiguration des Clients wird von folgender Umgebung ausgegangen:

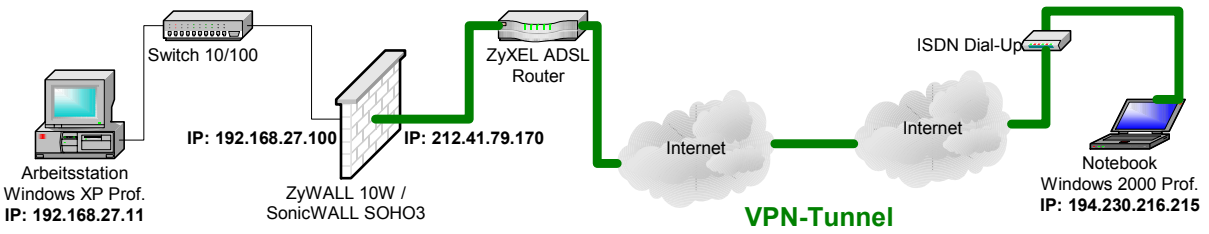


Abbildung 62: Versuchsumgebung für die Durchführung des VPN-Client-Tests

Auf den Firewalls wurden folgende Einstellungen vorgenommen:

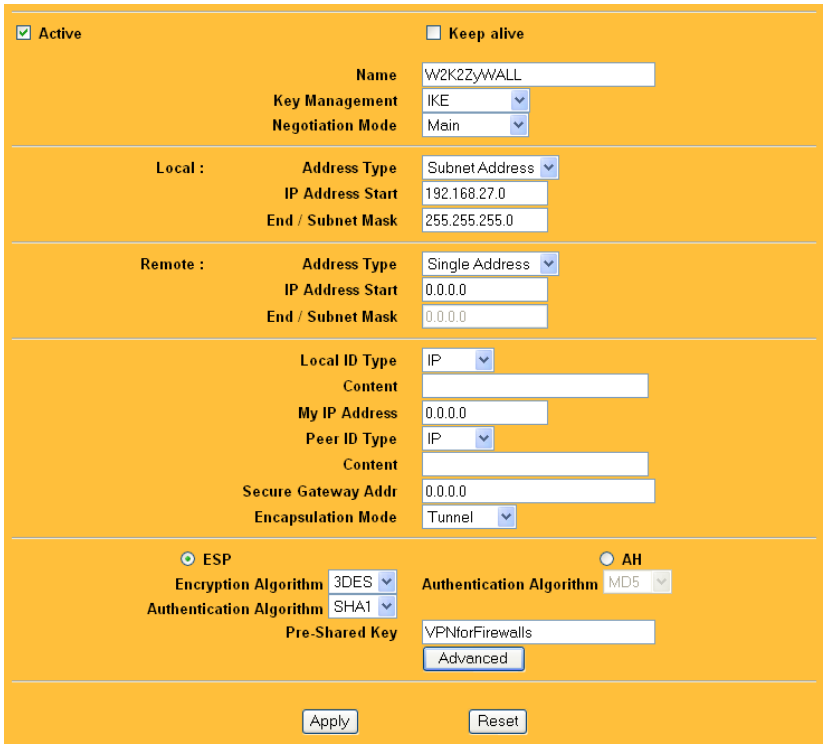


Abbildung 63: ZyWALL 10W – VPN-Grundeinstellungen für Windows 2000 IPSec-Client

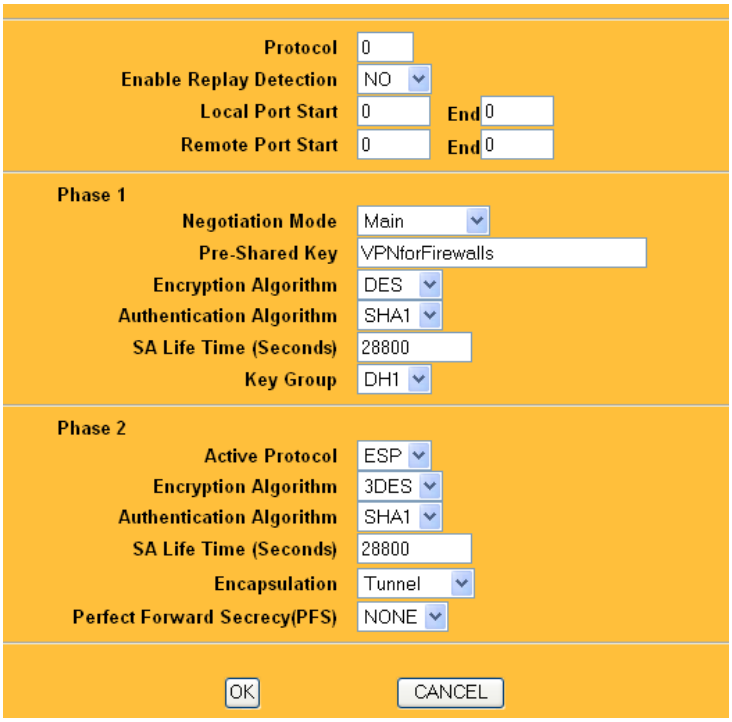


Abbildung 64: ZyWALL 10W – Erweiterte VPN-Einstellungen für Windows 2000 IPSec-Client

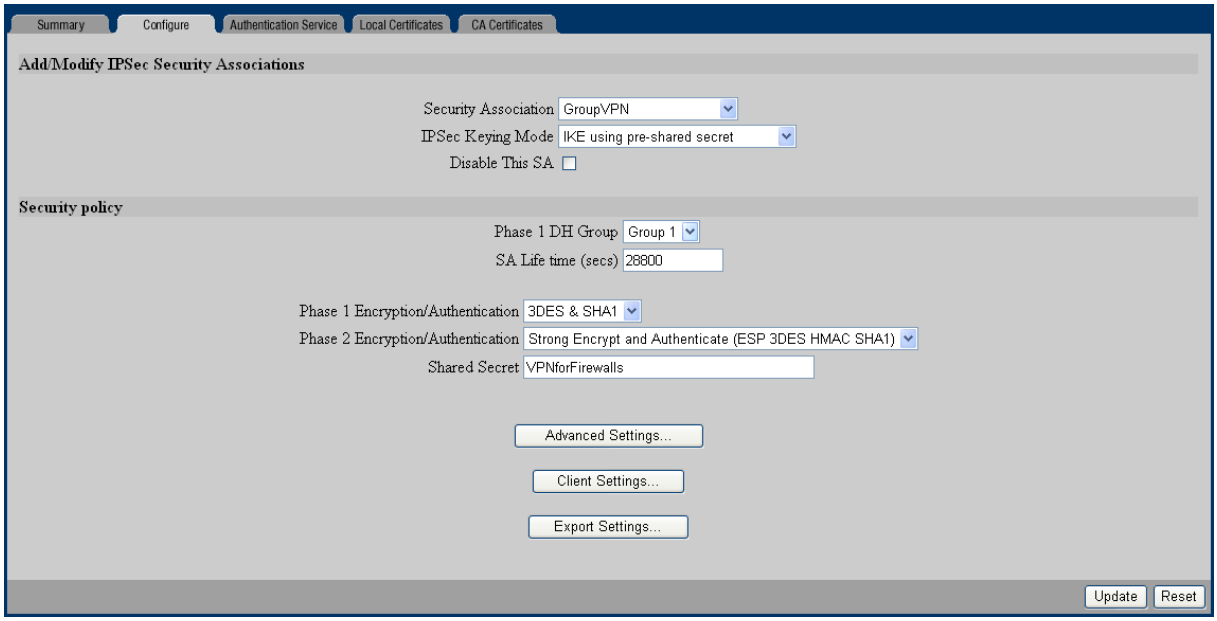
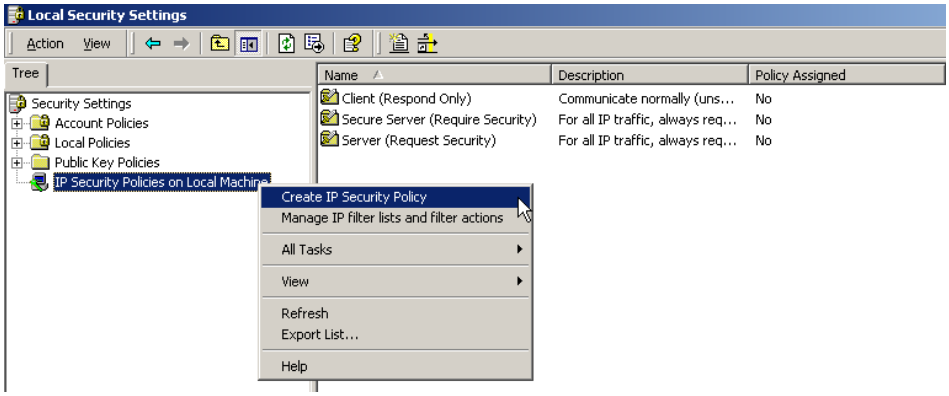
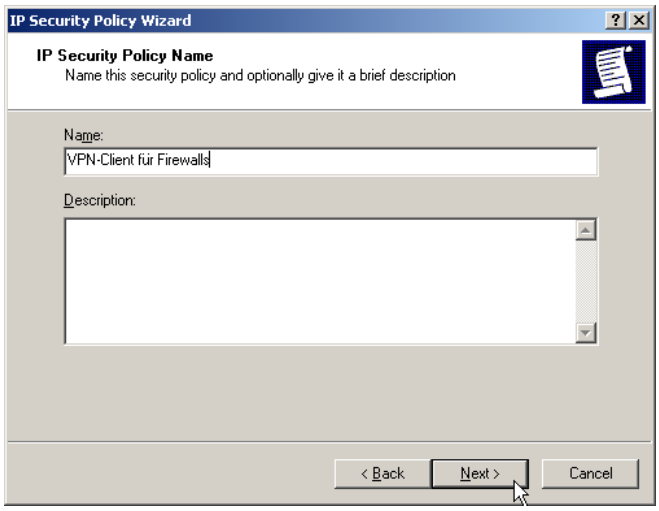


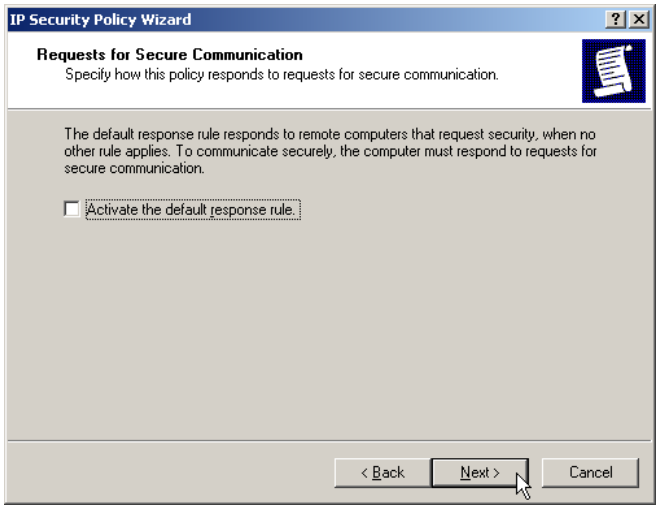
Abbildung 65: SonicWALL SOHO3 – VPN-Einstellungen für Windows 2000 IPSec-Client

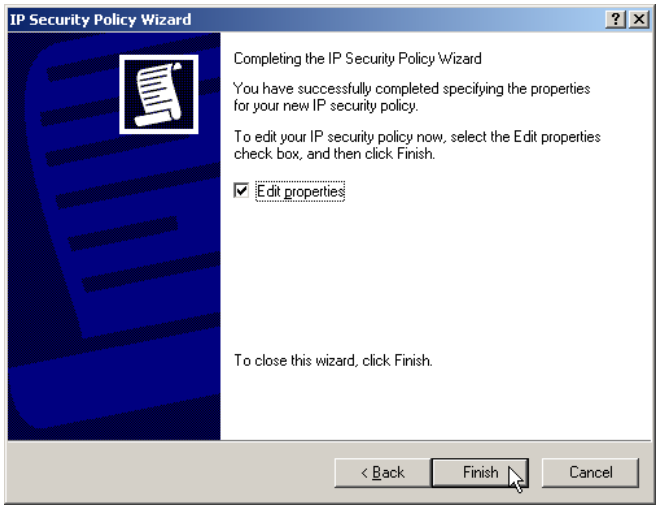
Die Einstellungen zur Check Point Firewall-1 NG und weitere Hinweise zum Windows 2000 IPSec-Zugriff auf diese Firewall sind in Kapitel 13.2.6 dokumentiert.

Um den VPN-Client einzurichten, müssen die lokalen Sicherheitseinstellungen von Windows 2000 aufgerufen werden. Dies erfolgt über „Start“ ⇨ „Ausführen…“ ⇨ „**`secpol.msc`**“. Danach sind folgende Einstellungen vorzunehmen:

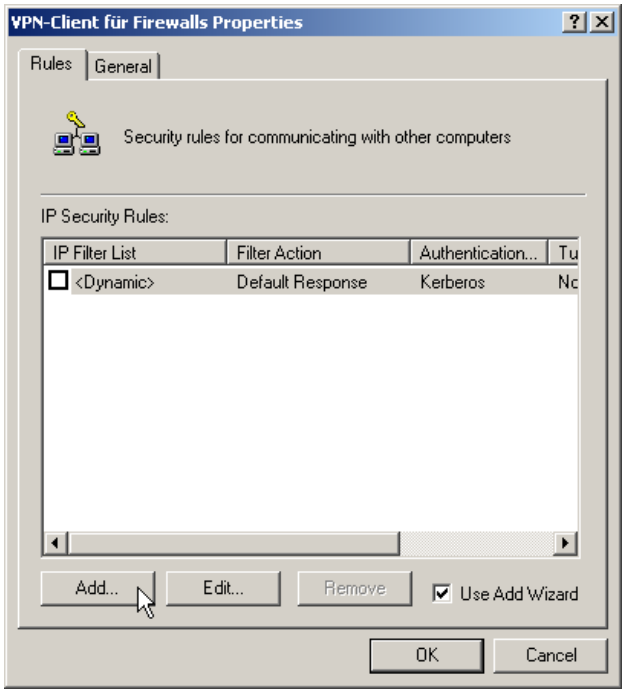

Local Security Settings
Action View
Tree
Security Settings
Account Policies
Local Policies
Public Key Policies
IP Security Policies on Local Machine
Name
Description
Policy Assigned
Client (Respond Only)
Communicate normally (uns...
No
Secure Server (Require Security)
For all IP traffic, always req...
No
Server (Request Security)
For all IP traffic, always req...
No
Create IP Security Policy
Manage IP filter lists and filter actions
All Tasks
View
Refresh
Export List...
Help


IP Security Policy Wizard
IP Security Policy Name
Name this security policy and optionally give it a brief description
Name:
VPN-Client für Firewalls
Description:
< Back
Next >
Cancel

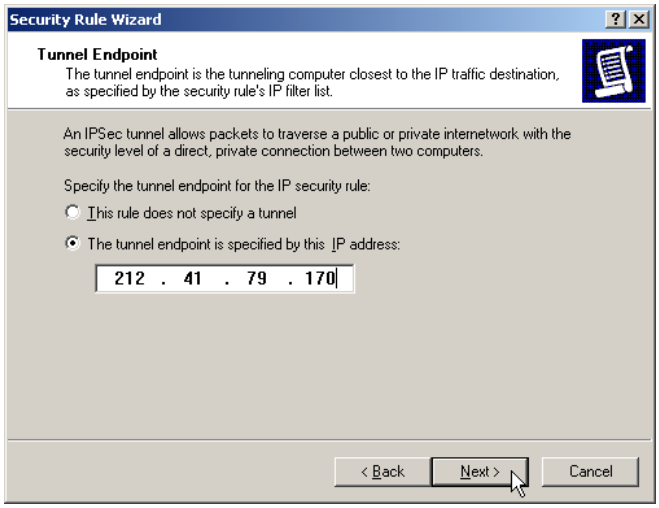

IP Security Policy Wizard
Requests for Secure Communication
Specify how this policy responds to requests for secure communication.
The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.
Activate the default response rule.
< Back
Next >
Cancel

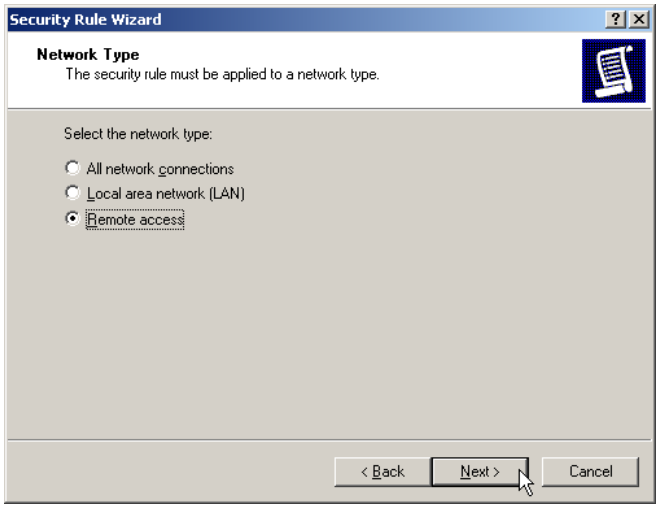

IP Security Policy Wizard
Completing the IP Security Policy Wizard
You have successfully completed specifying the properties for your new IP security policy.
To edit your IP security policy now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

VPN-Einstellungen, um vom VPN-Client auf die Firewall (resp. das interne Netzwerk) zuzugreifen

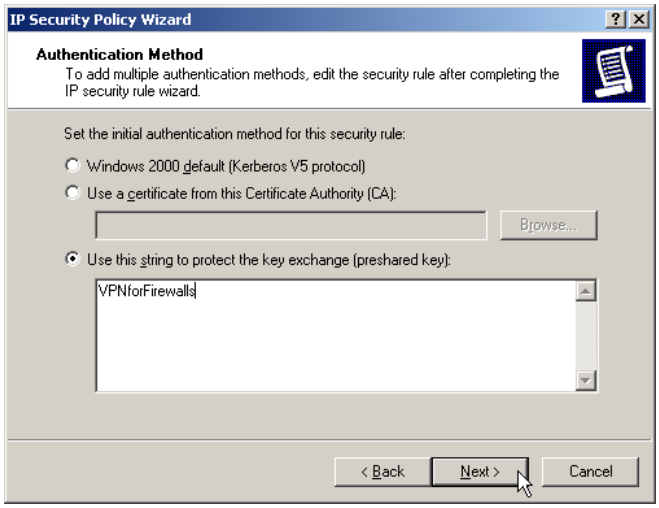


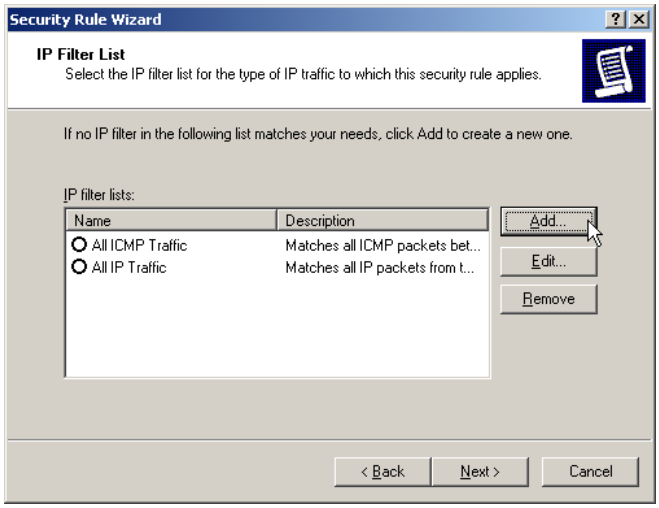
Bei der folgenden IP-Adresse handelt es sich um die öffentliche externe IP-Adresse (WAN-Interface) der Firewall, auf welche mittels VPN-Client zugegriffen werden soll:

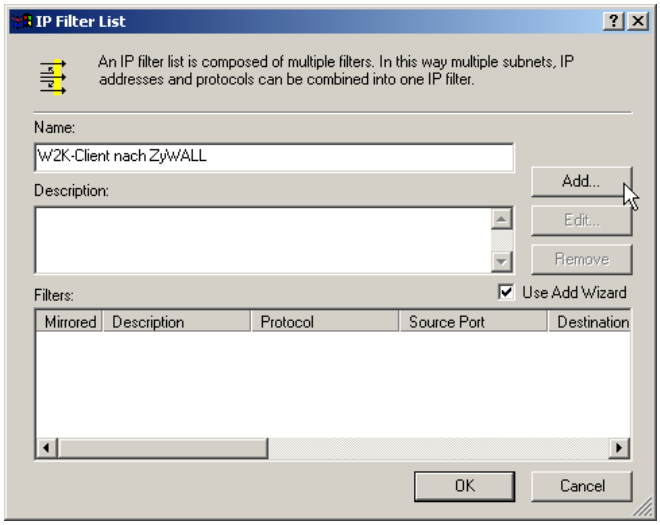

Security Rule Wizard
Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.
Specify the tunnel endpoint for the IP security rule:
This rule does not specify a tunnel
The tunnel endpoint is specified by this IP address:
212 . 41 . 79 . 170
< Back
Next >
Cancel

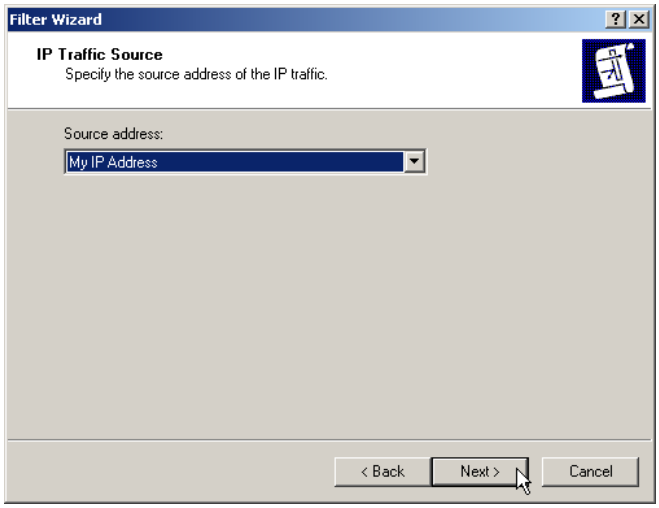


Der „Preshared Key“ muss mit den VPN-Einstellungen auf der Firewall übereinstimmen. Für die Anbindung an eine Check Point Firewall-1 NG FP 3 muss anstelle von „Preshared Keys“ mit digitalen Zertifikaten gearbeitet werden (siehe Ergänzungen in Kapitel 13.2.6):

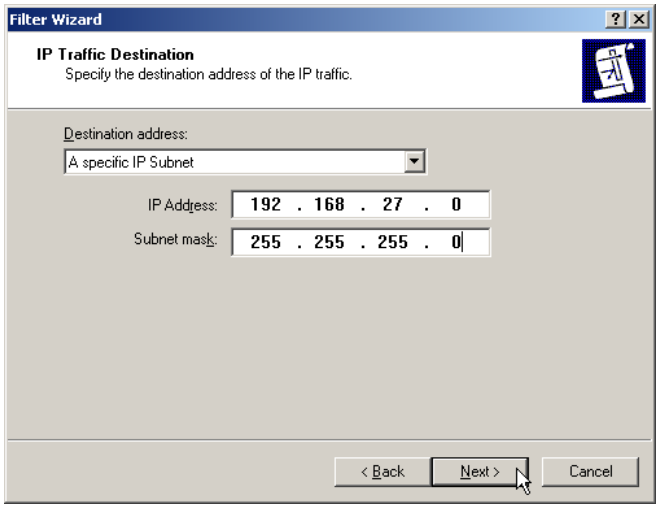

IP Security Policy Wizard
Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.
Set the initial authentication method for this security rule:
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this Certificate Authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
VPNforFirewalls
< Back
Next >
Cancel

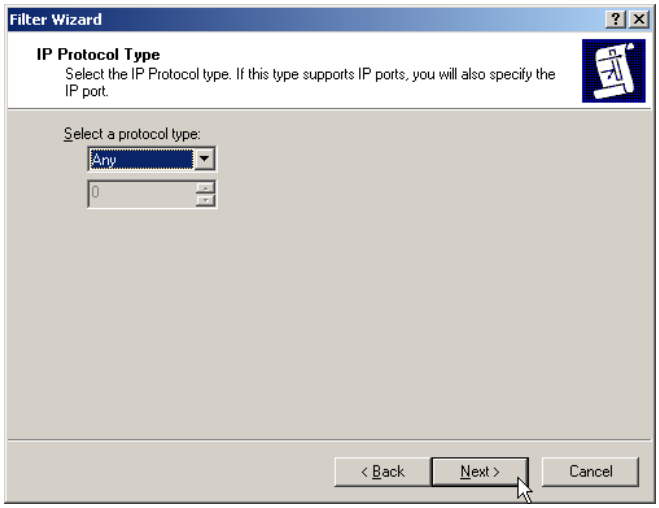

Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
Add...
Edit...
Remove
< Back
Next >
Cancel

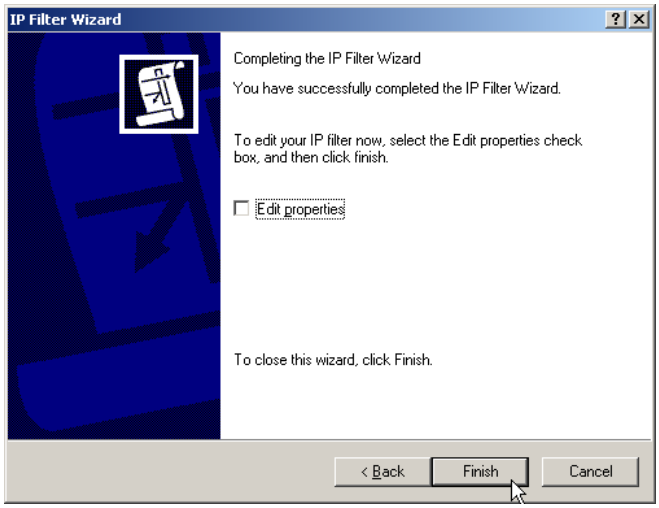


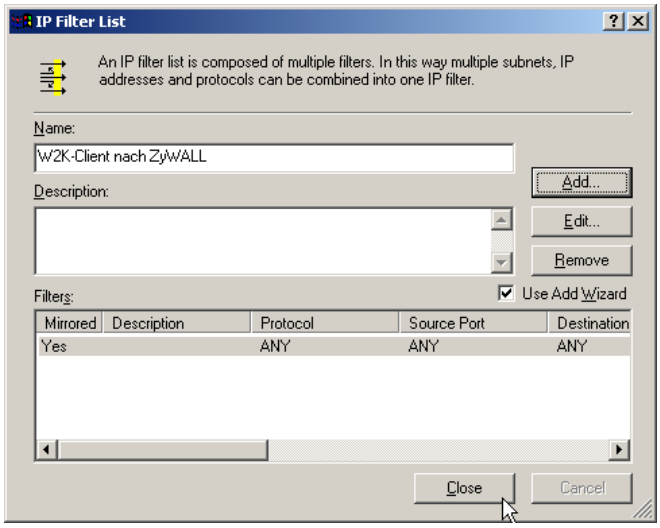


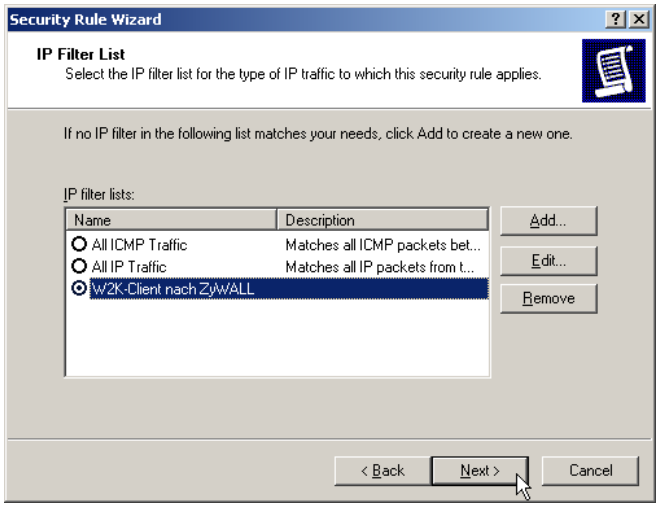
IP-Adressbereich des internen Netzwerkes hinter der Firewall:



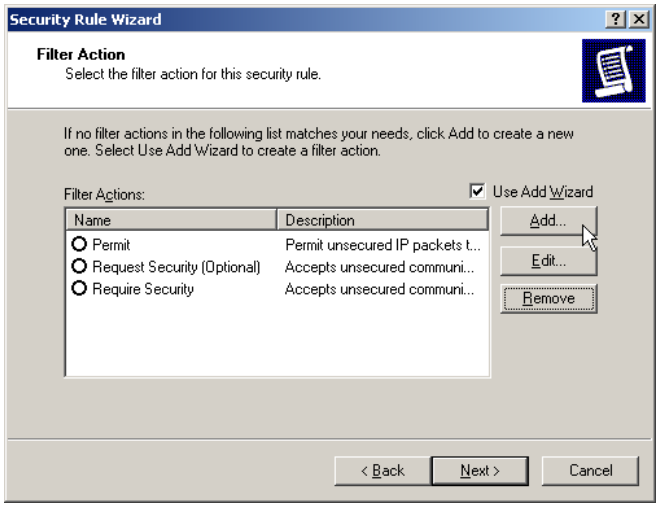

Filter Wizard
IP Protocol Type
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.
Select a protocol type:
Any
0
< Back
Next >
Cancel

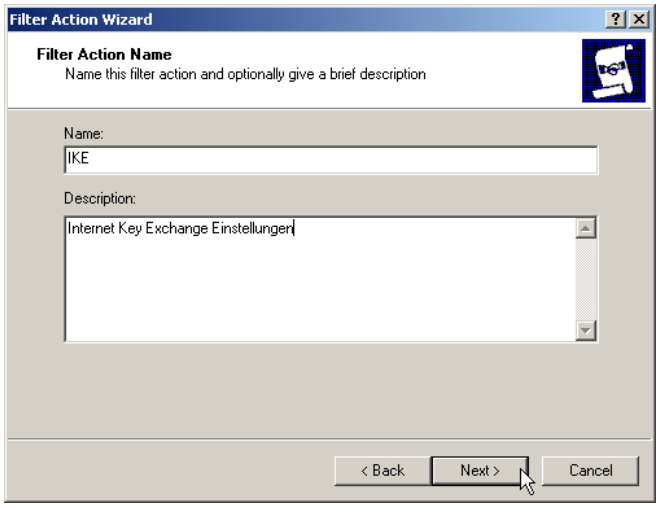

IP Filter Wizard
Completing the IP Filter Wizard
You have successfully completed the IP Filter Wizard.
To edit your IP filter now, select the Edit properties check box, and then click finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

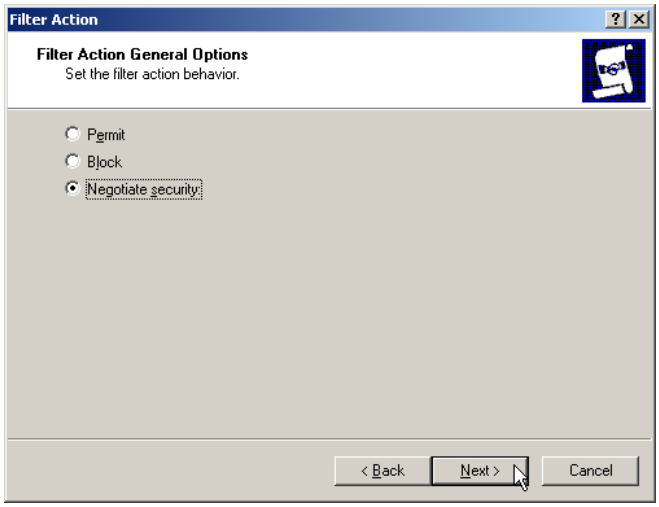

IP Filter List
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
W2K-Client nach ZyWALL
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
Yes
ANY
ANY
ANY
Close
Cancel

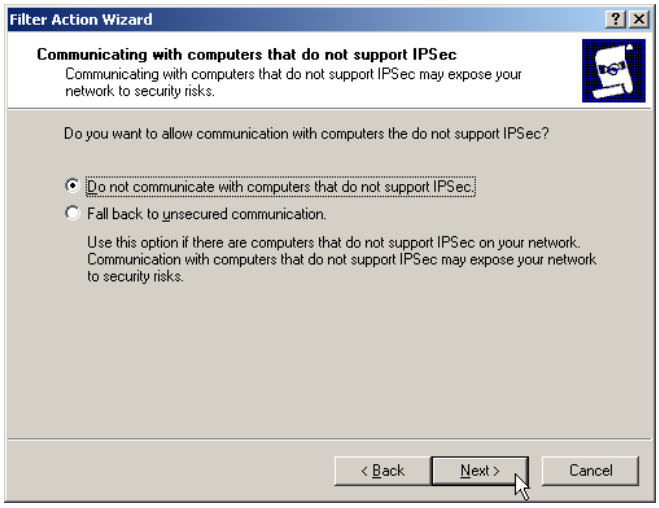

Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
W2K-Client nach ZyWALL
Add...
Edit...
Remove
< Back
Next >
Cancel

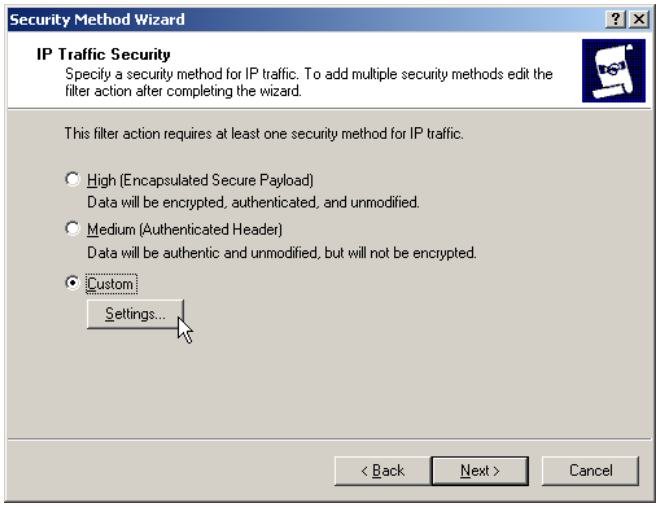
Einrichtung der IPSec-Protokolle





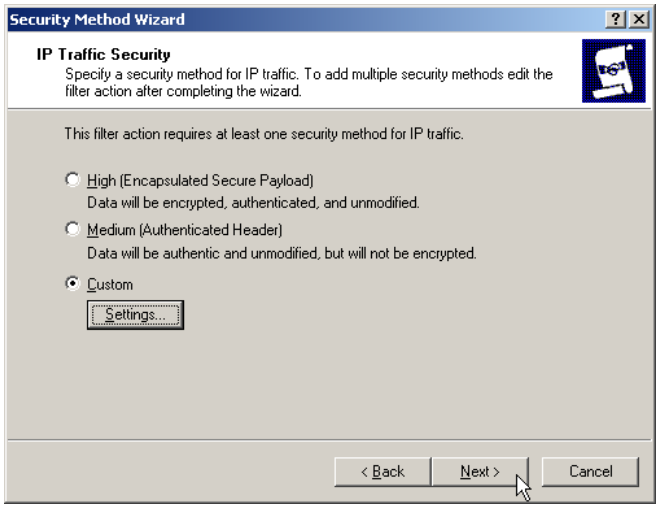


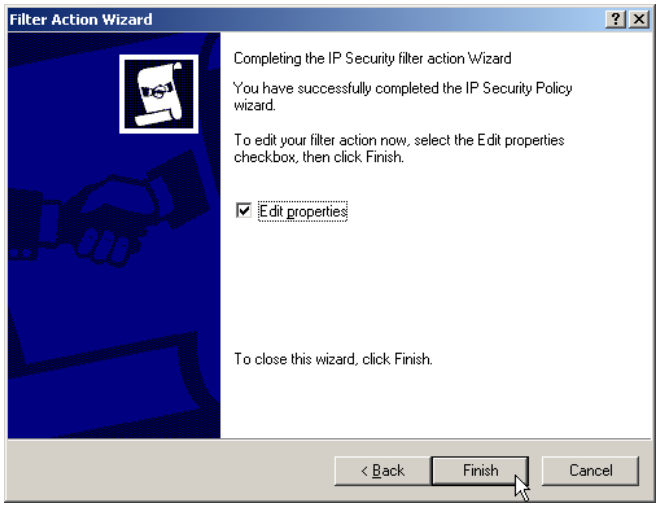

Filter Action Wizard
Communicating with computers that do not support IPSec
Communicating with computers that do not support IPSec may expose your network to security risks.
Do you want to allow communication with computers the do not support IPSec?
Do not communicate with computers that do not support IPSec.
Fall back to unsecured communication.
Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.
< Back
Next >
Cancel

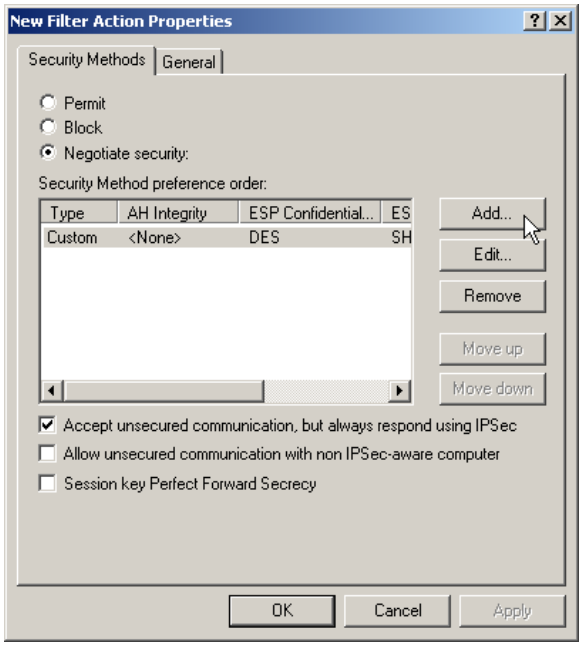

Security Method Wizard
IP Traffic Security
Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.
This filter action requires at least one security method for IP traffic.
High (Encapsulated Secure Payload)
Data will be encrypted, authenticated, and unmodified.
Medium (Authenticated Header)
Data will be authentic and unmodified, but will not be encrypted.
Custom
Settings...
< Back
Next >
Cancel

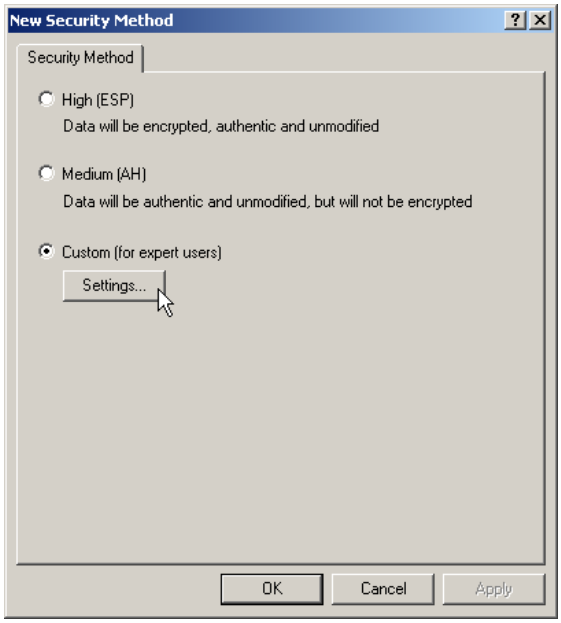
Einstellungen müssen den VPN-Einstellungen auf der Firewall entsprechen. Zur Auswahl stehen: MD5, SHA1, DES, 3DES.

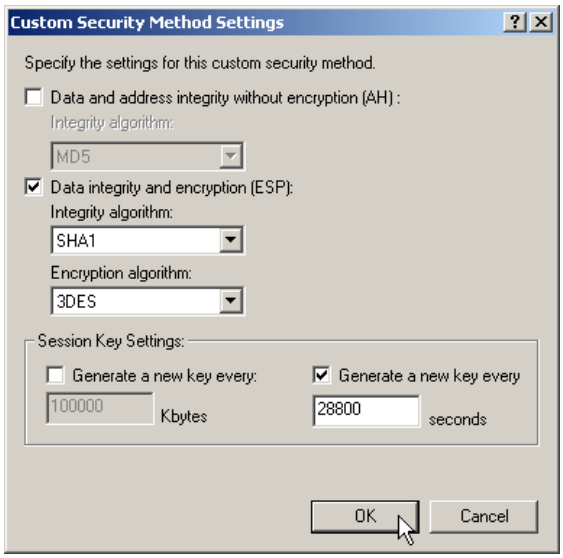
Falls für die Phase 1 und Phase 2 der IPSec-Security-Association auf der Firewall verschiedene Protokollkombinationen gewählt wurden, müssen diese auch hier alle abgebildet werden (in diesem Beispiel werden die Protokollkombinationen SHA1/DES und SHA1/3DES konfiguriert):

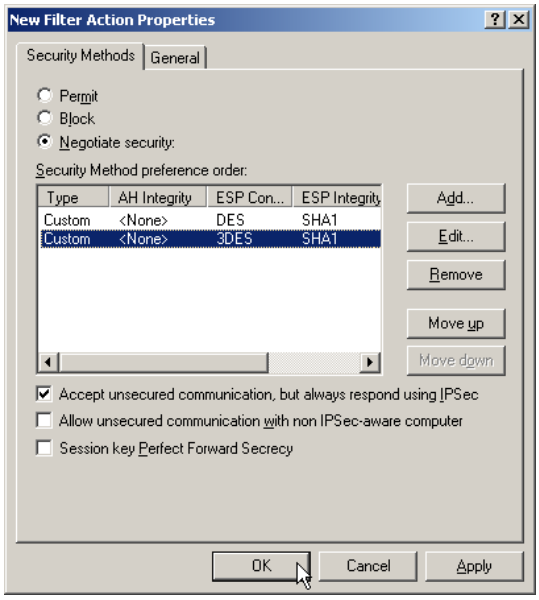

Security Method Wizard
IP Traffic Security
Specify a security method for IP traffic. To add multiple security methods edit the filter action after completing the wizard.
This filter action requires at least one security method for IP traffic.
High (Encapsulated Secure Payload)
Data will be encrypted, authenticated, and unmodified.
Medium (Authenticated Header)
Data will be authentic and unmodified, but will not be encrypted.
Custom
Settings...
< Back
Next >
Cancel

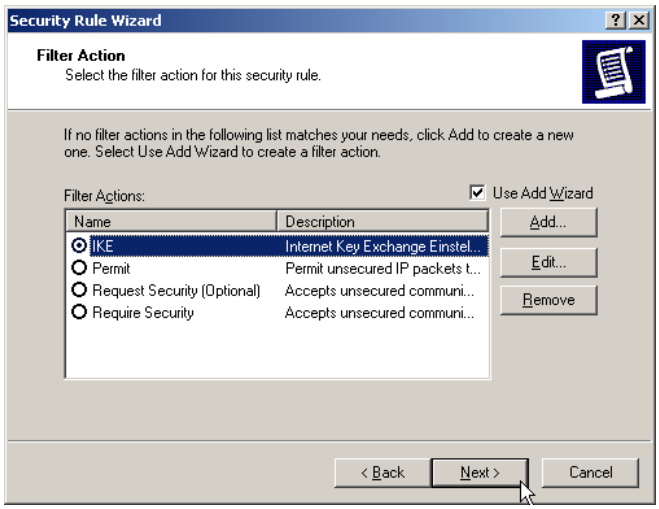

Filter Action Wizard
Completing the IP Security filter action Wizard
You have successfully completed the IP Security Policy wizard.
To edit your filter action now, select the Edit properties checkbox, then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

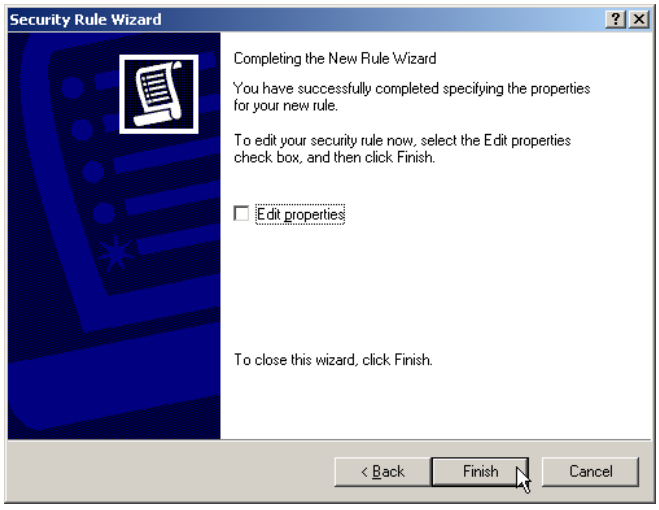

New Filter Action Properties
Security Methods
General
Permit
Block
Negotiate security:
Security Method preference order:
Type
AH Integrity
ESP Confidential...
ES
Custom
<None>
DES
SH
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non IPSec-aware computer
Session key Perfect Forward Secrecy
OK
Cancel
Apply

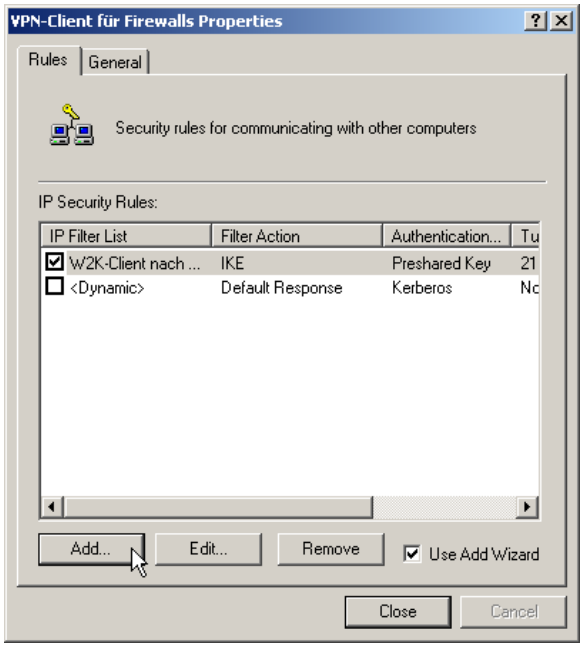

New Security Method
Security Method
High (ESP)
Data will be encrypted, authentic and unmodified
Medium (AH)
Data will be authentic and unmodified, but will not be encrypted
Custom (for expert users)
Settings...
OK
Cancel
Apply


Custom Security Method Settings
Specify the settings for this custom security method.
Data and address integrity without encryption (AH) :
Integrity algorithm:
MD5
Data integrity and encryption (ESP):
Integrity algorithm:
SHA1
Encryption algorithm:
3DES
Session Key Settings:
Generate a new key every:
100000
Kbytes
Generate a new key every
28800
seconds
OK
Cancel

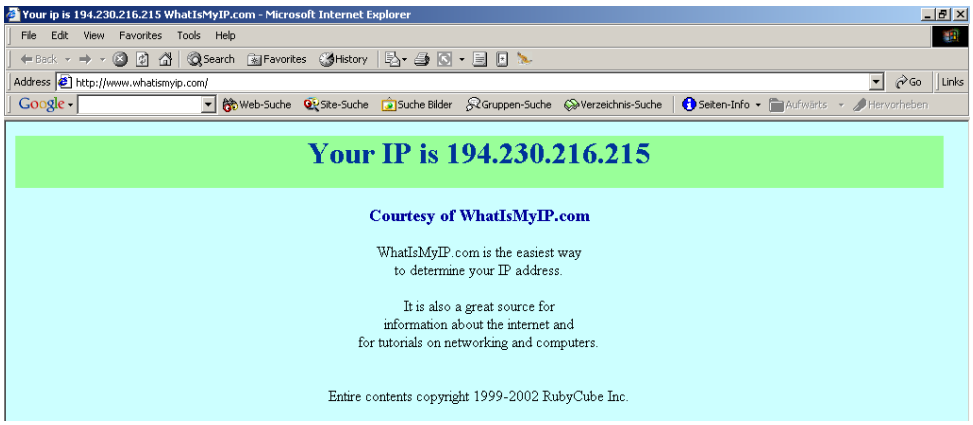

New Filter Action Properties
Security Methods
General
Permit
Block
Negotiate security:
Security Method preference order:
Type
AH Integrity
ESP Con...
ESP Integrity
Custom
<None>
DES
SHA1
Custom
<None>
3DES
SHA1
Add...
Edit...
Remove
Move up
Move down
Accept unsecured communication, but always respond using IPSec
Allow unsecured communication with non IPSec-aware computer
Session key Perfect Forward Secrecy
OK
Cancel
Apply


Security Rule Wizard
Filter Action
Select the filter action for this security rule.
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.
Filter Actions:
Use Add Wizard
Name
Description
IKE
Internet Key Exchange Einstel...
Permit
Permit unsecured IP packets t...
Request Security (Optional)
Accepts unsecured communi...
Require Security
Accepts unsecured communi...
Add...
Edit...
Remove
< Back
Next >
Cancel

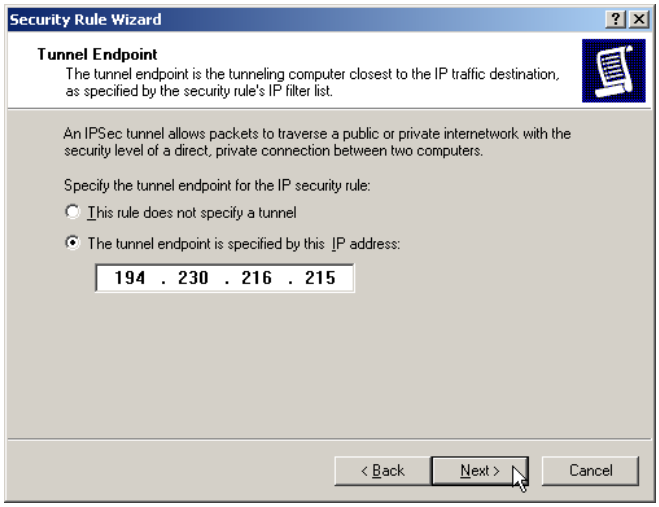

Security Rule Wizard
Completing the New Rule Wizard
You have successfully completed specifying the properties for your new rule.
To edit your security rule now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel

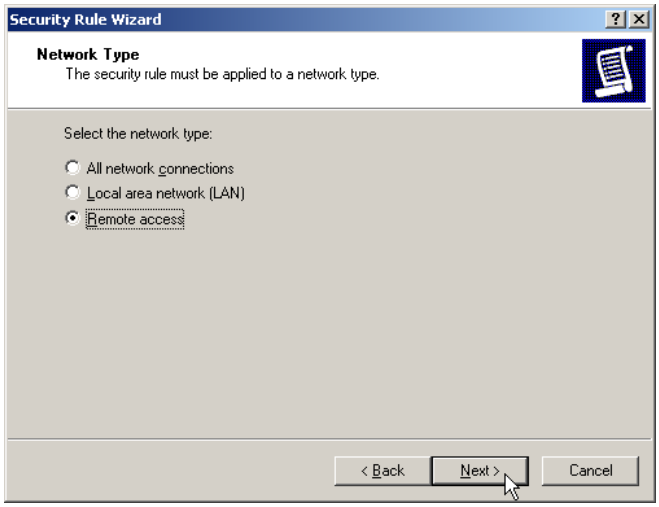


Aktuelle öffentliche IP-Adresse der Wählverbindung in Erfahrung bringen (z.B. über http://www.whatismyip.com):

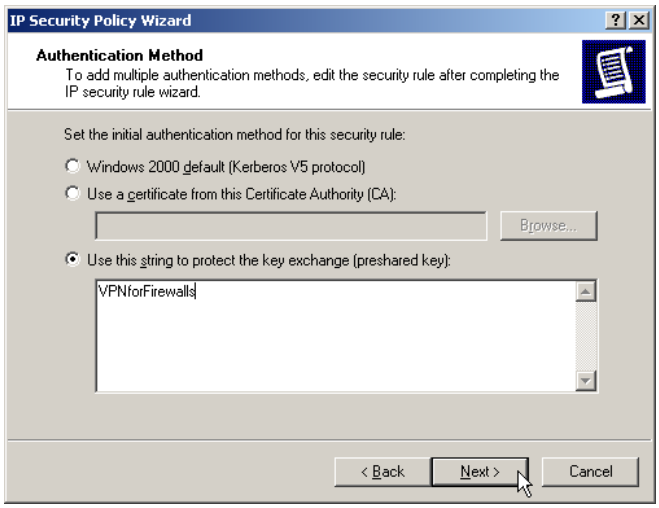

Your ip is 194.230.216.215 WhatIsMyIP.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.whatismyip.com/
Your IP is 194.230.216.215
Courtesy of WhatIsMyIP.com
WhatIsMyIP.com is the easiest way to determine your IP address.
It is also a great source for information about the internet and for tutorials on networking and computers.
Entire contents copyright 1999-2002 RubyCube Inc.

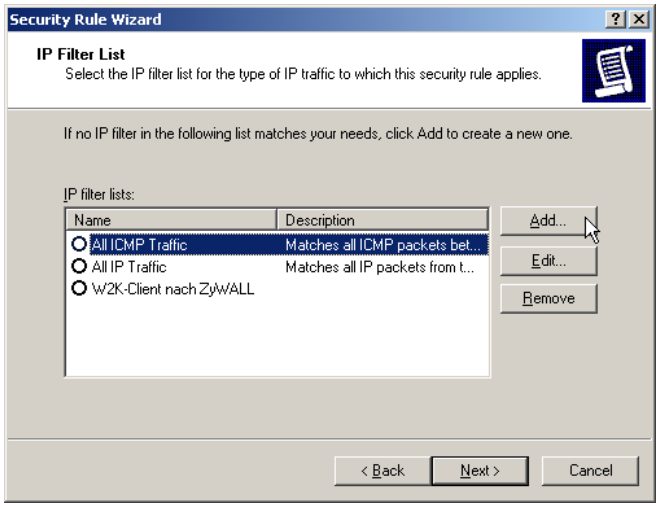
VPN-Einstellungen, um von der Firewall (resp. aus dem internen Netzwerk) zurück auf den VPN-Client zuzugreifen

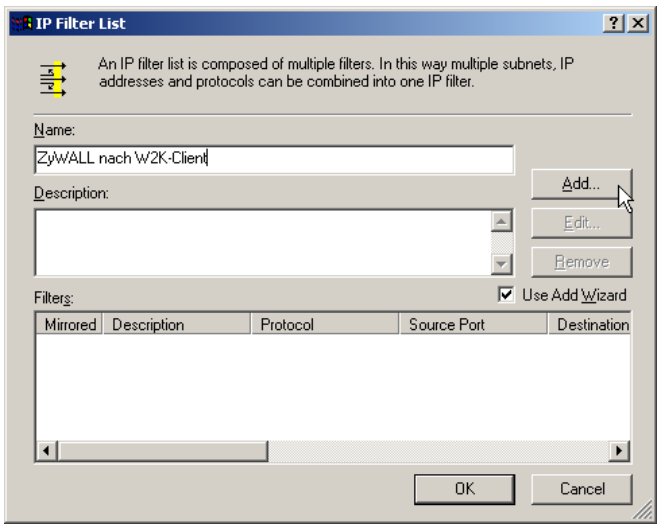

Security Rule Wizard
Tunnel Endpoint
The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.
An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.
Specify the tunnel endpoint for the IP security rule:
This rule does not specify a tunnel
The tunnel endpoint is specified by this IP address:
194 . 230 . 216 . 215
< Back
Next >
Cancel

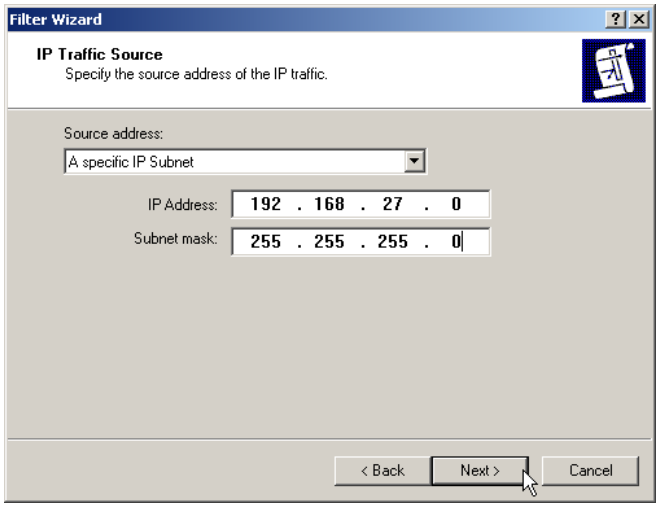


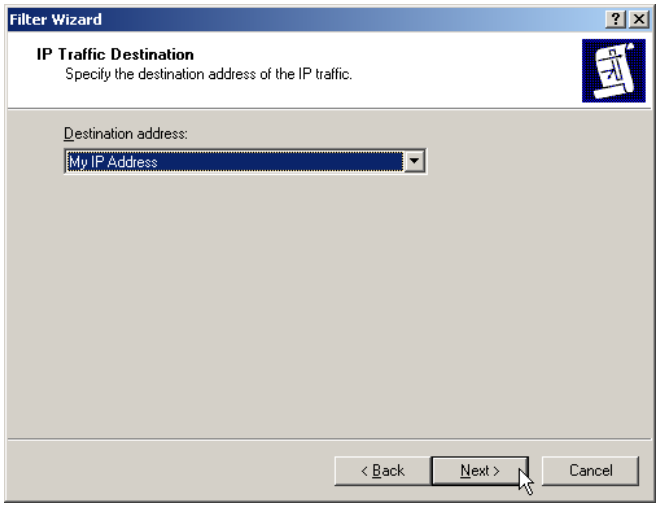
Der „Preshared Key“ muss wiederum den bereits vorgenommen Einstellungen entsprechen:

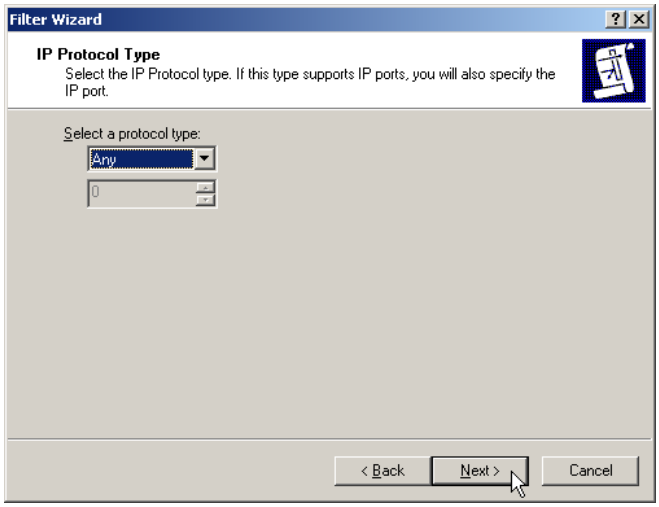

IP Security Policy Wizard
Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.
Set the initial authentication method for this security rule:
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this Certificate Authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
VPNforFirewalls
< Back
Next >
Cancel

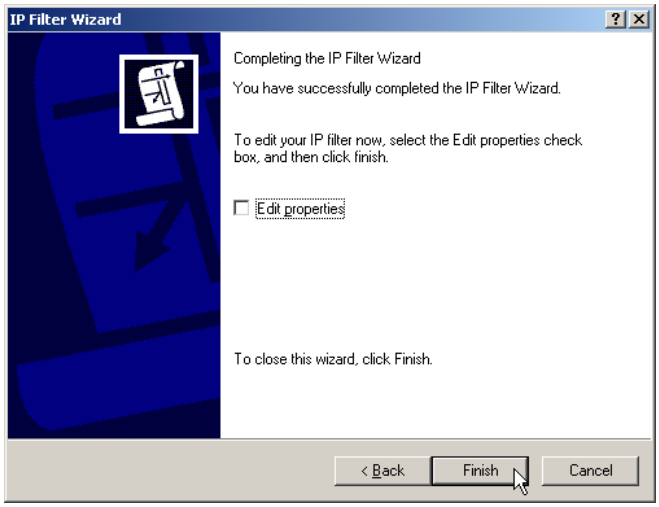

Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
W2K-Client nach ZyWALL
Add...
Edit...
Remove
< Back
Next >
Cancel

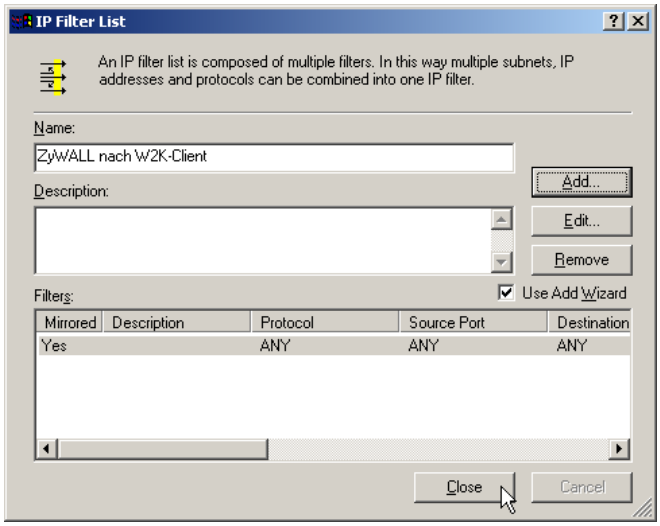

IP Filter List
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
ZyWALL nach W2K-Client
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
OK
Cancel

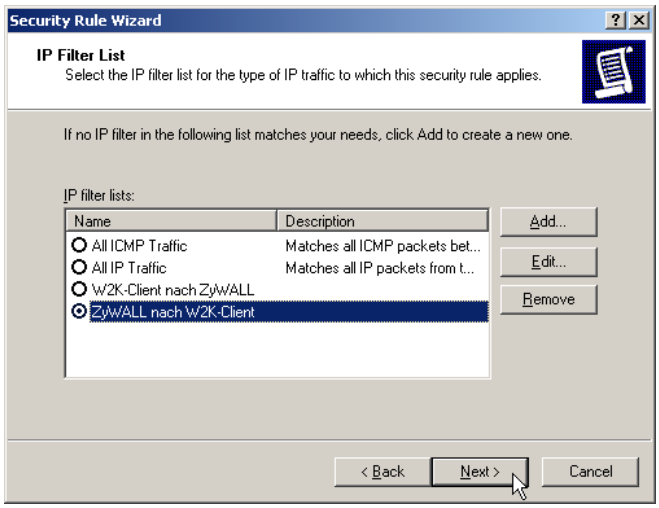

Filter Wizard
IP Traffic Source
Specify the source address of the IP traffic.
Source address:
A specific IP Subnet
IP Address:
192 . 168 . 27 . 0
Subnet mask:
255 . 255 . 255 . 0
< Back
Next >
Cancel

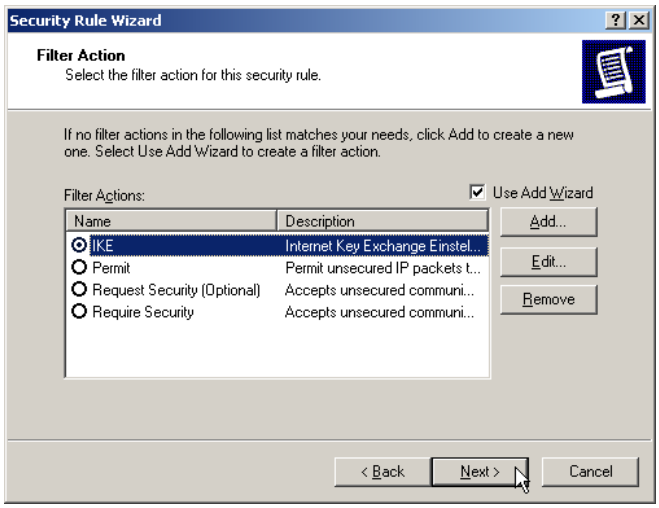

Filter Wizard
IP Traffic Destination
Specify the destination address of the IP traffic.
Destination address:
My IP Address
< Back
Next >
Cancel

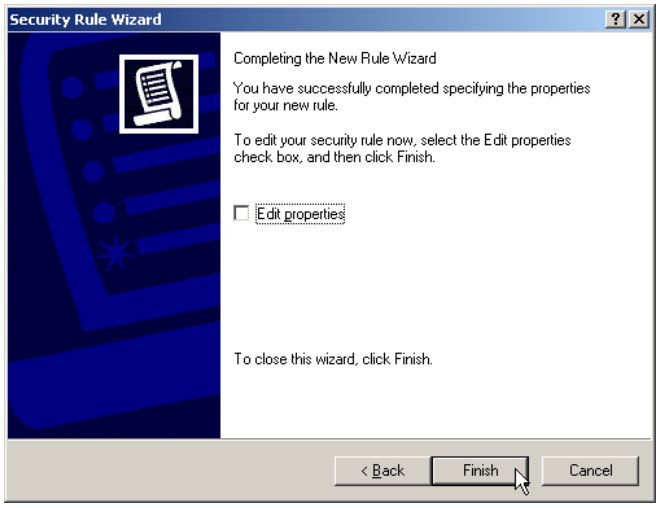

Filter Wizard
IP Protocol Type
Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.
Select a protocol type:
Any
0
< Back
Next >
Cancel

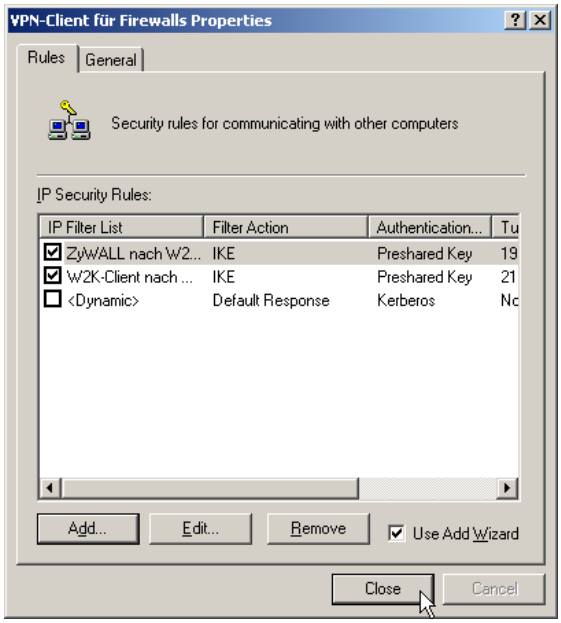

IP Filter Wizard
Completing the IP Filter Wizard
You have successfully completed the IP Filter Wizard.
To edit your IP filter now, select the Edit properties check box, and then click finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel


IP Filter List
An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.
Name:
ZyWALL nach W2K-Client
Description:
Add...
Edit...
Remove
Filters:
Use Add Wizard
Mirrored
Description
Protocol
Source Port
Destination
Yes
ANY
ANY
ANY
Close
Cancel

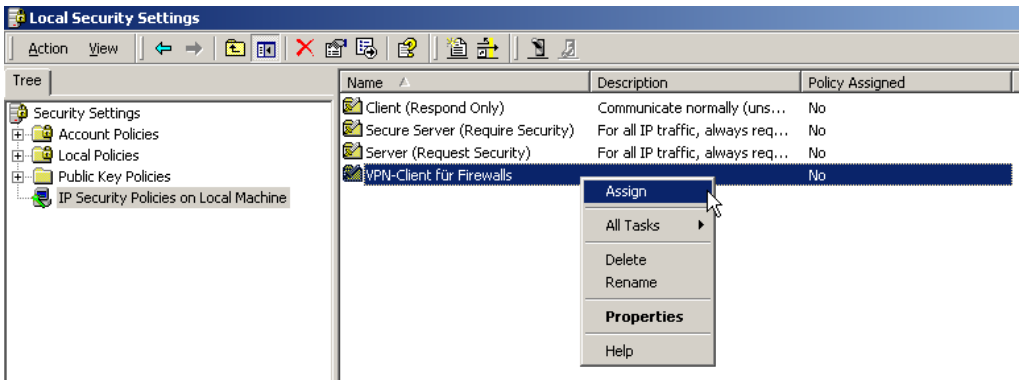

Security Rule Wizard
IP Filter List
Select the IP filter list for the type of IP traffic to which this security rule applies.
If no IP filter in the following list matches your needs, click Add to create a new one.
IP filter lists:
Name
Description
All ICMP Traffic
Matches all ICMP packets bet...
All IP Traffic
Matches all IP packets from t...
W2K-Client nach ZyWALL
ZyWALL nach W2K-Client
Add...
Edit...
Remove
< Back
Next >
Cancel


Security Rule Wizard
Filter Action
Select the filter action for this security rule.
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.
Filter Actions:
Use Add Wizard
Name
Description
IKE
Internet Key Exchange Einstel...
Permit
Permit unsecured IP packets t...
Request Security (Optional)
Accepts unsecured communi...
Require Security
Accepts unsecured communi...
Add...
Edit...
Remove
< Back
Next >
Cancel

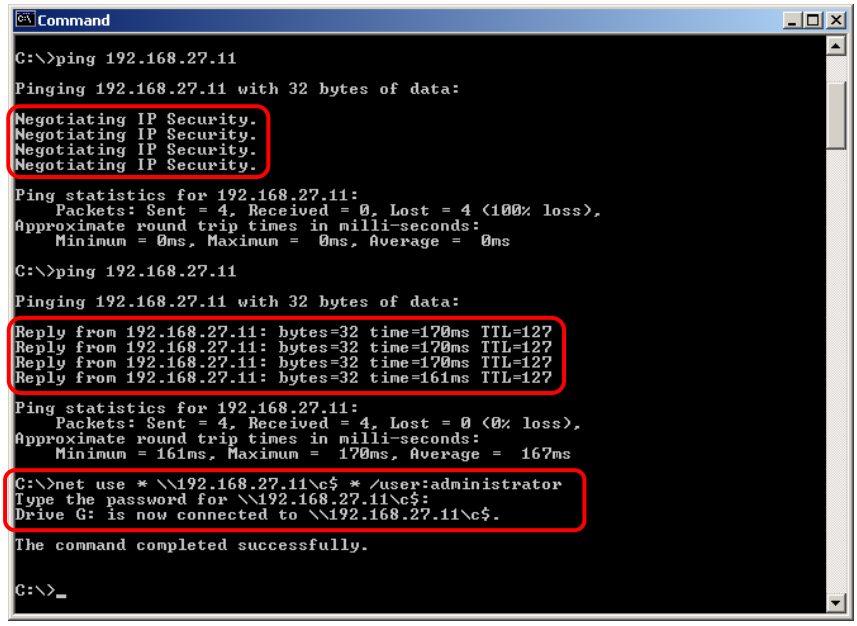

Security Rule Wizard
Completing the New Rule Wizard
You have successfully completed specifying the properties for your new rule.
To edit your security rule now, select the Edit properties check box, and then click Finish.
Edit properties
To close this wizard, click Finish.
< Back
Finish
Cancel



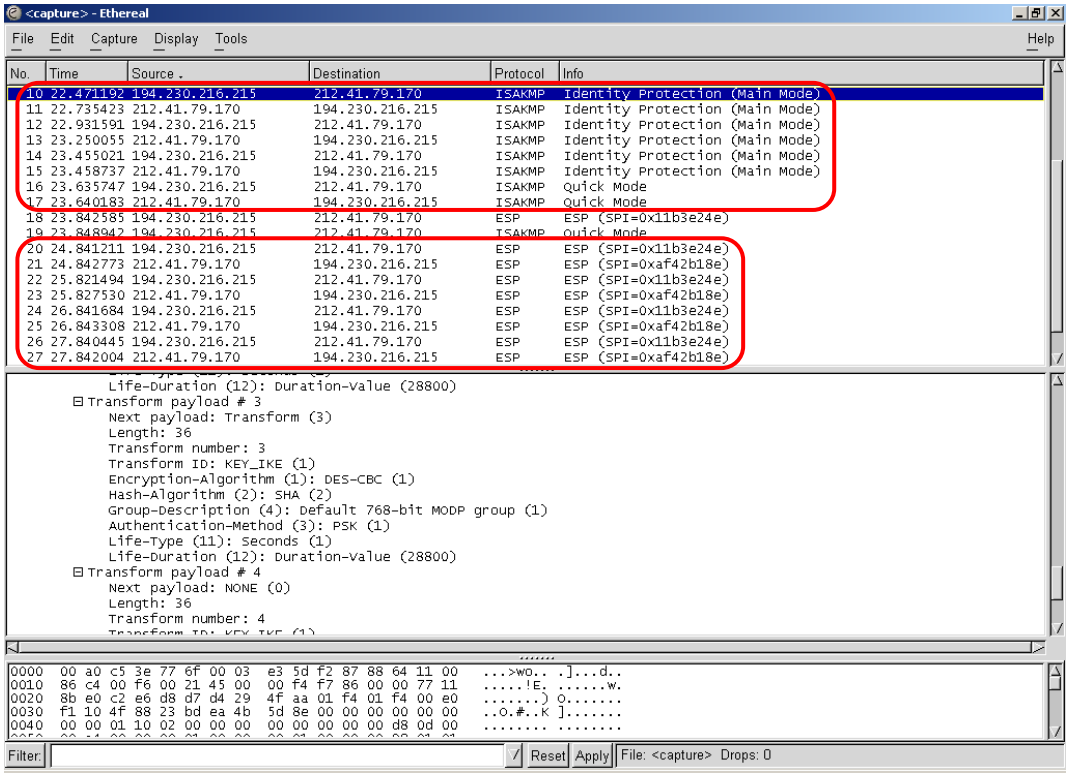
Nun müssen die Einstellungen aktiviert werden:



Beim ersten Ping-Versuch vom VPN-Client auf ein internes System hinter der Firewall werden die zu verwendenden VPN-Protokolle ausgehandelt. Der zweite Ping-Versuch führt dann bereits zum Erfolg und es lassen sich mit dem VPN-Client-System freigegebene Verzeichnisse auf dem internen System anbinden:


Command
C:\>ping 192.168.27.11
Pinging 192.168.27.11 with 32 bytes of data:
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Ping statistics for 192.168.27.11:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.27.11
Pinging 192.168.27.11 with 32 bytes of data:
Reply from 192.168.27.11: bytes=32 time=170ms TTL=127
Reply from 192.168.27.11: bytes=32 time=170ms TTL=127
Reply from 192.168.27.11: bytes=32 time=170ms TTL=127
Reply from 192.168.27.11: bytes=32 time=161ms TTL=127
Ping statistics for 192.168.27.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 161ms, Maximum = 170ms, Average = 167ms
C:\>net use * \\192.168.27.11\c$ * /user:administrator
Type the password for \\192.168.27.11\c$:
Drive G: is now connected to \\192.168.27.11\c$.
The command completed successfully.
C:\>

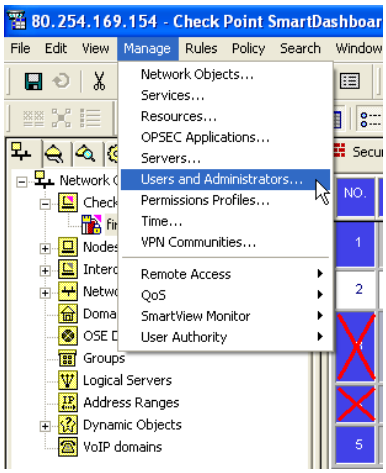
Die Verkehrsanalyse mit dem Sniffer zeigt die durchgeführte Security Association (ISAKMP-Pakete ⇨ Internet Security Association and Key Management Protocol) und den verschlüsselten Datenverkehr (ESP-Pakete ⇨ Encapsulating Security Payload):



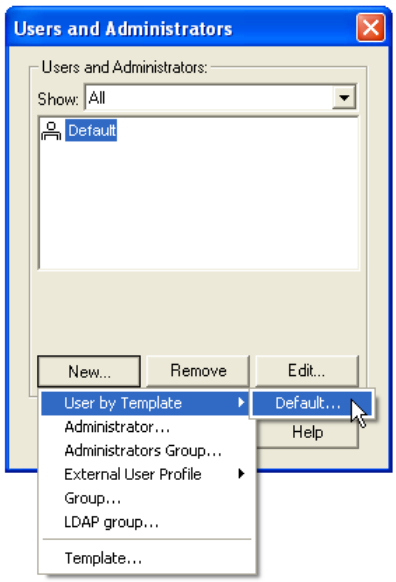
13.2.6 Windows 2000 IPSec – Ergänzungen zum Einrichten des VPN-Clients für Check Point Firewalls

Auf der Check Point Firewall-1 NG FP 3 müssen folgende Einstellungen vorgenommen werden:

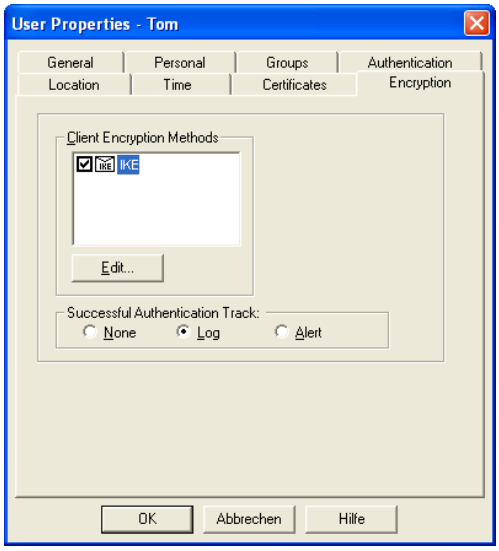
- Aktivierung des VPN-Moduls „VPN-1 Pro“ in den „General Properties“ der Firewall
- Allfällige Anpassung der VPN-Grundeinstellungen im Bereich „Remote Access“, „VPN – Basic“ und „VPN – Advanced“ (3DES und SHA1) der „Global Properties“
- Erfassen der Benutzer und Benutzergruppen unter „Manage“ ⇨ „Users and Administrators…“:



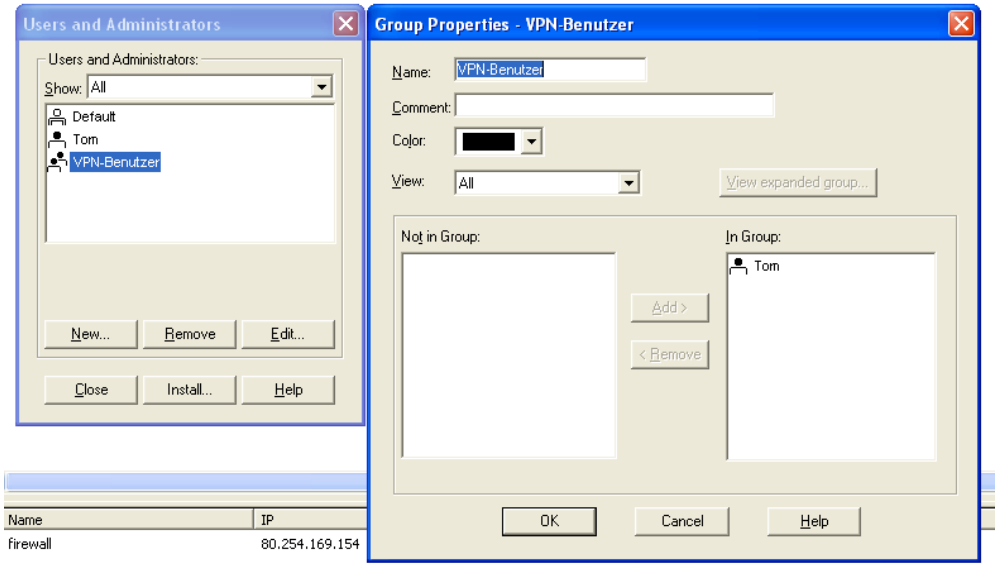
- Zumindest einen Benutzer und eine Benutzergruppe erfassen:



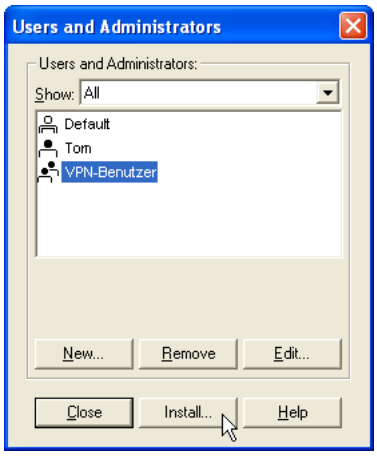
- Bei der Benutzererfassung insbesondere unter den Registern „Authentication“ (z.B. „VPN-1 & Firewall-1 Password“), „Encryption“ („IKE“ aktivieren ⇨ Authentication „Public Key“) und „Certificates“ („Generate and save“) die entsprechenden Einstellungen vornehmen und das digitale Benutzerzertifikat speichern:



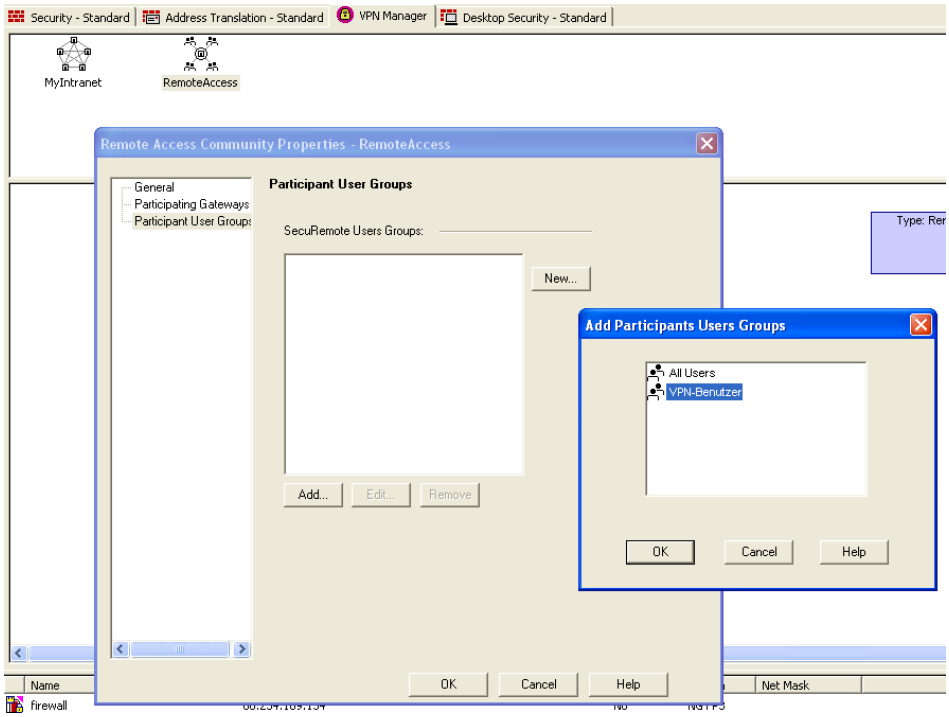
- Neue Benutzergruppe erfassen und erstellten Benutzer hinzufügen:



- Neu erfasste Benutzer und Benutzergruppen auf der Firewall installieren:



- Beim „VPN Manager“ mittels Doppelklick auf das Objekt „RemoteAccess“ die erstellte Benutzergruppe als VPN-Remote-Access partizipierende Gruppe hinzufügen:



- Ebenfalls unter „Remote Access“ im Bereich „Participating Gateways“ das Firewall-Objekt hinzufügen

- Folgendes Objekt erstellen:
  - Objekt-Typ „Network“ ⇨ Name „Internes_Netz“ ⇨ Netzwerk-Adresse „172.16.0.0“ ⇨ Netzmaske „255.255.255.0“ ⇨ Broadcast-Adresse „included“ ⇨ NAT „Hide Mode“

Damit die VPN-Benutzer Zugriff auf die internen Systeme haben, müssen auf der Firewall noch die entsprechenden Firewall-Regeln erfasst und aktiviert werden. Es gilt zu beachten, dass für den VPN-Client-Zugriff eigentlich nur die Firewall-Regel Nr. 2 benötigt wird:

Security - Standard | Address Translation - Standard | VPN Manager | Desktop Security - Standard

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL
1	Any	firewall	Any	Any	drop	Log	Policy Ta
2	Any	Internes_Netz	RemoteAccess	Any	accept	Log	Policy Ta
3	Internes_Netz	Any	Any	Any	accept	None	Policy Ta
4	Any	Any	Any	Any	drop	Log	Policy Ta

Erläuterungen zu den abgebildeten Regeln

Nr.	Erläuterungen
1	Auf die Firewall kann nicht zugegriffen werden (so genannte Stealth-Regel)
2	Alle Verbindungen, welche Bestandteil der VPN-Community „RemoteAccess“ sind (siehe „IF VIA“), können auf die Systeme im internen Netzwerk zugreifen. Da die zuvor erfasste Benutzergruppe zur VPN-Community „RemoteAccess“ gehört, können alle Benutzer, welche dieser Benutzergruppen angehören, auf die internen Systeme zugreifen

3 Alle internen Systeme dürfen überallhin Verbindungen aufnehmen

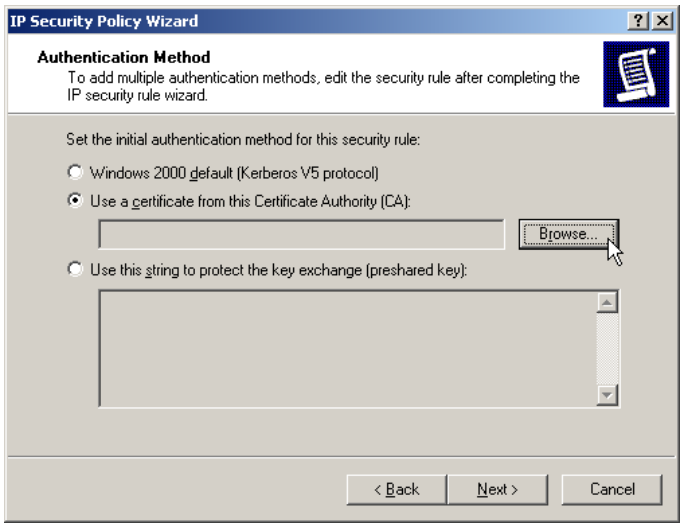
4 Alle übrigen Zugriffsversuche von irgendwoher nach irgendwohin werden geblockt

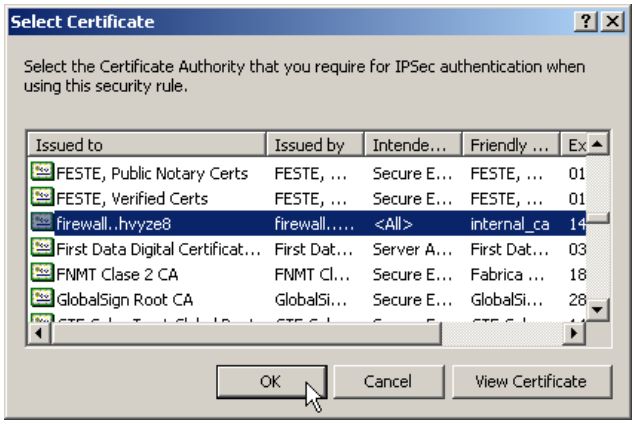
Auf dem Windows 2000 System, auf welchem der IPSec-VPN-Client eingerichtet werden soll, muss nun das zuvor auf der Check Point Firwall-1 generierte Zertifikat importiert werden:

- Menu „Start“ ⇨ „Ausführen…“ ⇨ „mmc“ (Management-Konsole starten)
- Menu „Datei“ ⇨ „Snap-In hinzufügen/entfernen…“ ⇨ Schalfläche „Hinzufügen“
- „Zertifikate“ auswählen ⇨ Schaltfläche „Hinzufügen“ ⇨ „Computerkonto“ ⇨ Schaltfläche „Weiter“ ⇨ „Lokalen Computer“ ⇨ Schaltfläche „Fertig stellen“ ⇨ Schalfläche „Schliessen“ ⇨ Schalfläche „OK“
- Rechte Maustaste auf „Eigene Zertifikate“ ⇨ „Alle Tasks“ ⇨ „Importieren…“
- Erstelltes Zertifikat auswählen und importieren (Passwort eingeben, privaten Schlüssel als exportierbar markieren, Zertifikatsspeicher automatisch auswählen)

Abweichungen zur Einrichtung des Windows 2000 IPSec-Clients gegenüber den Ausführungen in Kapitel 13.2.5:

Anstelle der Eingabe eines „Preshared Keys“, wird das selbstsignierte Root-Zertifikat des zuvor importieren Benutzerzertifikats ausgewählt (hier wurde das Zertifikat auf den Namen „firewall..hvyze8“ ausgestellt; „firewall“ kommt deshalb im Namen vor, weil das Firewall-Objekt unter Check Point so benannt wurde):


IP Security Policy Wizard
Authentication Method
To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.
Set the initial authentication method for this security rule:
Windows 2000 default (Kerberos V5 protocol)
Use a certificate from this Certificate Authority (CA):
Browse...
Use this string to protect the key exchange (preshared key):
< Back
Next >
Cancel



Die übrigen Schritte zur Einrichtung des VPN-Clients erfolgen entsprechend der Hinweise unter Kapitel 13.2.5.

Erklärung des Autors

Ich erkläre hiermit, dass ich die vorliegende Arbeit resp. die von mir ausgewiesene Leistung selbständig, ohne Mithilfe Dritter und nur unter Benützung der angegebenen Quellen verfasst habe. Das Urheberrecht der Arbeit liegt beim Verfasser. Das Institut für Wirtschaftsinformatik hat ein internes Nutzungsrecht.

Thun, 12. Juni 2003

Tom Schmidt _____